Kacper Gradoń

MOŻLIWOŚCI TAKTYCZNEGO WYKORZYSTANIA OTWARTYCH ŹRÓDEŁ INFORMACJI W INTERNECIE PRZEZ ORGANA ŚCIGANIA ORAZ SPRAWCÓW PRZESTĘPSTW I ZAMACHÓW TERRORYSTYCZNYCH

Opportunities for the tactical use of the Internet-based open-source information by the law-enforcement agencies, criminal offenders and terrorists

Pojęcie otwartych źródeł informacji ugruntowane jest w fachowej literaturze przedmiotu (kryminalistycznej, policyjnej, wojskowej, związanej z bezpieczeństwem wewnętrznym), a zakres znaczeniowy tego terminu (i jego synonimów, takich jak np. „biały wywiad" czy niejednokrotnie wykorzystywane w polskim piśmiennictwie anglojęzyczne określenie *Open Source Intelligence* – OSInt) nie budzi większych wątpliwości. Chociaż niniejsze opracowanie nie ma na celu zaprezentowania ewolucji pojęć ani historii rozwoju metod wywiadowczych, należy jednak przedstawić definicje terminu przyjęte na potrzeby dalszego wywodu. Korzystać zatem będę z przyjętej międzynarodowo siatki pojęciowej, w tym:

1. definicji NATO, według której biały wywiad (określany mianem „danych wywiadowczych ze źródeł jawnych/OSINT" – *open source intelligence/ renseignement de source ouverte*) to „dane wywiadowcze pochodzące zarówno z publicznie dostępnych informacji, jak i innych jawnych informacji o ograniczonym rozpowszechnianiu lub dostępie"[1];
2. definicji Armii Stanów Zjednoczonych, która konkretyzuje pojęcia „otwartego źródła" (definiowanego jako „osoba lub grupa osób dostarczająca informację i nieoczekująca zachowania jej prywatności") i „informacji dostępnej publicznie" (definiowanej jako „dane, fakty, instrukcje lub inne materiały opublikowane lub rozpowszechnione ogółowi społeczeństwa; dostępne na prośbę obywatela; legalnie zauważone lub usłyszane przez dowolnego przypadkowego obserwatora; udostępnione na spotkaniu otwartym dla ogółu społeczeństwa")[2].

[1] Słownik Terminów i Definicji NATO zawierający terminy wojskowe i ich definicje stosowane w NATO. AAP-6 (2014), s. 288, http://www.wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf.
[2] Open Source Intelligence ATP 2-22.9, Headquarters, Department of the Army. Army Techniques Publication FMI 2-22.9, Washington D.C. 10.07.2012, s. 1-1, http://www.fas.org/irp/doddir/army/atp2-22-9.pdf.

Warto podkreślić, że w polskiej literaturze dotyczącej tej tematyki (która notabene jest – w stosunku do zakresu zastosowań otwartych źródeł informacji – relatywnie skromna) przyjmuje się najczęściej polskojęzyczne warianty definicji zagranicznych lub pisze po prostu o „legalnym zdobywaniu informacji z przestrzeni publicznej”[3]. Co znamienne, również autorzy jedynej wydanej do tej pory w Polsce monografii poświęconej szeroko rozumianemu białemu wywiadowi unikają podawania własnej definicji problemu stanowiącego temat ich publikacji: pisząc o białym wywiadzie i *open source intelligence*, zaznaczają, że nie przyjęli jednej definicji tych terminów, a „był to zabieg celowy, aby pokazać różnorodność problemów i punktów widzenia na opisywane w pracy metody wykorzystywania otwartych źródeł informacji. (…) praca ma stanowić wstęp do dyskusji nad tymi metodami w praktyce podmiotów z sektora publicznego i prywatnego”[4].

W literaturze poświęconej klasyfikacji źródeł informacji o charakterze otwartym wymienia się najczęściej następujące lokalizacje danych:

1. media: gazety codzienne, periodyki, audycje radiowe i telewizyjne, media elektroniczne (Internet);
2. dane publiczne: raporty rządowe, dane oficjalne (budżety, dane demograficzne), wystąpienia oficjalne, debaty legislacyjne, konferencje prasowe, przemówienia;
3. źródła profesjonalne i akademickie: konferencje, sympozja, informacje korporacji zawodowych, artykuły naukowe, oświadczenia ekspertów[5].

Powyższa systematyka jest oczywiście uproszczona i można ją dowolnie rozwijać, tworząc dalsze podziały i podtypy. Przykładowo przyjęty w polskich źródłach podział wylicza:

1. media tradycyjne, w szczególności agencje prasowe, gazety, czasopisma, książki, radio (z zastrzeżeniem, że źródła te zawierają autorskie komentarze do danych w postaci wywiadów z ekspertami, analizy i śledztwa dziennikarskie);
2. Internet (media elektroniczne) – portale agencji informacyjnych, blogi, fora, portale społecznościowe, organizacje pozarządowe, think tanki i inne;
3. usługi komercyjne – informacje udostępniane przez prywatne podmioty trudniące się zbieraniem informacji;
4. inne usługi w zakresie dostarczania danych;
5. literaturę niszową – analizy, informacje z sektora akademickiego i organizacji pozarządowych, trudniejsze w dostępie ze względu na ograniczony zasięg i zakres;
6. opinie ekspertów, naukowców, uczestników zdarzeń;

[3] B. Sienkiewicz, *Historia pewnego złudzenia*, „Przegląd Bezpieczeństwa Wewnętrznego ABW. Wydanie specjalne” 2012, s. 52.

[4] W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, C.H. Beck, Warszawa 2012, s. 15.

[5] M.M. Lowenthal, *Intelligence. From Secrets to Policy*, fourth edition, CQ Press, Washington D.C. 2009, s. 103.

7. bazy zdjęć i obrazów (satelitarne obrazowanie powierzchni ziemi)[6].

Aktualnie, ze względu na dominującą we współczesnym świecie rolę mediów elektronicznych i nowoczesnych technologii informatycznych wykorzystujących bezpośrednio bądź pośrednio narzędzia internetowe lub z nimi powiązanych, coraz większą wagę zyskuje komponent internetowych źródeł informacji o charakterze białego wywiadu. Już przeszło dekadę temu podkreślano, że otwarte źródła internetowe są gwałtownie rosnącym obszarem zainteresowania instytucji wywiadowczych[7], a obecnie tendencja ta w wyraźny sposób zyskała na intensywności. Świadczy o tym m.in. potrzeba dalszych klasyfikacji usadowionych w strukturze Internetu źródeł danych. Jeszcze kilka lat temu wystarczające było uznanie „Internetu" za samoistną kategorię w szeregu otwartych źródeł informacji, jednak coraz częściej mamy do czynienia z tworzeniem bardziej szczegółowych typologii. Wymienia się zatem źródła takie jak:

1. serwisy informacyjne, portale, wortale;
2. blogi (dzienniki internetowe) – w tym pamiętniki internetowe, fotoblogi, wideoblogi, blogi muzyczne, blogi korporacyjne i organizacyjne, blogi tematyczne, mikroblogi;
3. fora internetowe i listy dyskusyjne;
4. otwarte serwisy chat i IRC;
5. serwisy społecznościowe;
6. inne rodzaje źródeł internetowych, w tym strony domowe, bazy danych, serwisy aukcyjne i z ogłoszeniami drobnymi, sieci wymiany plików i sieć głęboką[8].

Niektórzy autorzy rozbudowują katalog otwartych źródeł informacji dostępnych w Internecie, wymieniając ponad 20 podkategorii (internetowe wydania gazet i czasopism, blogi i mikroblogi, portale społecznościowe, grupy dyskusyjne, grupy informacyjne, komunikatory internetowe, serwisy typu Wiki, serwisy wideo, serwisy fotograficzne, strony internetowe organizacji pozarządowych, strony internetowe przedsiębiorców, rządowe strony internetowe, rządowe dokumenty udostępnione w ramach informacji publicznej, newslettery, reklamy internetowe, publikacje patentowe i aplikacje patentowe, rejestry domen WhoIs, internetowe stacje radiowe, telewizje internetowe, serwisy mapowe, serwisy zdjęć satelitarnych, serwisy zdjęć lotniczych)[9].

Warto zauważyć, że zaproponowane wyżej podziały nie mogą i nie powinny w żadnym razie stanowić katalogu zamkniętego – wraz z rozwojem technologii i w związku z powstaniem nowych narzędzi i usług internetowych bez wątpienia pojawią się nowe kategorie źródeł, dotychczas nieprzewidywane, a co najwyżej

[6] P. Chlebowicz, *Biały wywiad z perspektywy kryminalistyki*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 60.

[7] H. Fergusson, *Spy: A Handbook*, Bloomsbury Publishing, London 2004, s. 81.

[8] P. Maciołek, *Internet a OSINT – szanse i praktyczne zastosowania*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 225–230.

[9] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011, s. 62–63.

antycypowane w ramach analizy strategicznej trendów w budowie nowych aplikacji i platform. Jest to w gruncie rzeczy poważny problem, z którym dotychczas nie spotykaliśmy się w takiej skali i natężeniu. Obrazuje to już sam wzrost liczby urządzeń podłączonych do Internetu: w 1988 roku do sieci podłączonych było ok. sześćdziesięciu tysięcy urządzeń informatycznych (wśród nich nieliczne komputery osobiste)[10], natomiast w chwili obecnej[11] według danych firmy informatycznej CISCO na całym świecie podłączonych do Internetu jest ponad szesnaście miliardów osób, procesów logicznych i urządzeń – średnio co sekundę liczba ta rośnie o około 120 jednostek, a przewidywania CISCO mówią o ponad 50 miliardach jednoczesnych połączeń z Internetem w roku 2020. Ilustruje to licznik Cisco Connections Counter[12].

Najpopularniejsza obecnie sieć społecznościowa Facebook posiadała pod koniec pierwszego roku swojego istnienia (2004) około miliona użytkowników[13], natomiast w pierwszym kwartale 2015 roku Facebook miał już prawie półtora miliarda aktywnych użytkowników[14]. Podobny fenomen wzrostu zanotowała platforma mikroblogowa Twitter, która po pierwszym roku (2006) swojego funkcjonowania miała ok. 16 tysięcy użytkowników, a w pierwszym kwartale 2015 r. już ponad trzysta milionów[15]. Powstała w październiku 2010 r. sieć społecznościowa Instagram (obecnie własność korporacji Facebook), służąca przede wszystkim do publikowania i wymiany fotografii, miała pod koniec 2010 r. ok. miliona użytkowników, natomiast po czterech latach (grudzień 2014 r.) ich liczba wzrosła do ponad trzystu milionów[16].

Zilustrowana powyżej bezprecedensowa skala wzrostu, z jaką mamy do czynienia w przypadku Internetu i powiązanych z nim platform i technologii, niewątpliwie świadczy o tym, że w hierarchii otwartych źródeł informacji Internet zajmuje obecnie zdecydowane pierwsze miejsce, a trend ten nie wydaje się możliwy do zatrzymania czy odwrócenia (co najwyżej możemy się spodziewać jego spowolnienia). Fakt ten zauważają praktycy – funkcjonariusze organów ścigania i instytucji wywiadowczych.

Przeprowadzone przez W. Filipkowskiego na przełomie 2010 i 2011 roku badania dwóch grup funkcjonariuszy Policji nt. zagadnień związanych z białym wywiadem wykazały, że w owym czasie Internet (rozumiany jako źródło informacji w białym wywiadzie) wymieniany był (w zależności od grupy badanej) na drugim lub trzecim miejscu (po prasie i tzw. ogóle mediów) – wskazało go odpowiednio 21% i 17% respondentów. Pytania szczegółowe dotyczące przydatności informacji

[10] J. Zittrain, *The Future of the Internet and How to Stop It*, Penguin Books, 2009, s. 36.

[11] Tj. w czerwcu 2015 r. – uwaga ta jest istotna ze względu na tempo rozwoju infrastruktury sieciowej.

[12] http://blogs.cisco.com/news/cisco-connections-counter (dostęp 12.06.2015 r.).

[13] http://finance.yahoo.com/news/number-active-users-facebook-over-years--214600186--finance.html (dostęp 10.06.2015 r.).

[14] http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users--worldwide/ (dostęp 10.06.2015 r.).

[15] http://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/ (dostęp 10.06. 2015 r.).

[16] http://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/ (dostęp 10.06.2015 r.).

pozyskiwanych z Internetu przy wykonywaniu obowiązków służbowych spotkały się z dużym uznaniem respondentów (średnio ok. 88% odpowiedzi wskazywało na to, że takie informacje są „bardzo przydatne" lub „przydatne")[17]. W odniesieniu do działalności służb specjalnych monitorowanie i wyszukiwanie przez sieć internetową jest obecnie najpowszechniejszą metodą pozyskiwania przez Agencję Bezpieczeństwa Wewnętrznego jawnych źródeł i informacji[18].

W 2014 i 2015 roku przeprowadziliśmy (K. Gradoń i A. Gutkowska) wywiady i badania ankietowe związane ze zwalczaniem ekstremizmu i terroryzmu tzw. „samotnych wilków" w ramach realizowanego przez nas projektu Siódmego Programu Ramowego Komisji Europejskiej FP7 PRIME[19]. Jednym z aspektów naszych badań było zdiagnozowanie, czy informacje z białego wywiadu, ze szczególnym uwzględnieniem źródeł internetowych, stanowią istotne narzędzie pracy instytucji odpowiedzialnych za zwalczanie przedmiotowych zagrożeń. Badania przeprowadziliśmy m.in. wśród przedstawicieli polskiej Policji, Straży Granicznej i Agencji Bezpieczeństwa Wewnętrznego, policji brytyjskiej, amerykańskiej (NYPD), hiszpańskiej oraz przedstawicieli EUROPOL-u. Dodatkowo samodzielnie przeprowadziłem podobne badania na grupie 80 policjantów indyjskich (w stopniu nie niższym od pułkownika)[20]. Aktualnie kompleksowe wyniki badań poddawane są szczegółowej analizie, jednak warto zaznaczyć, że jeśli chodzi o aspekt istotności internetowych źródeł otwartych w pracy funkcjonariuszy organów ścigania, praktycznie wszyscy respondenci (97,5%) wymieniali Internet jako kluczowe miejsce pozyskiwania informacji (wśród źródeł otwartych).

Bezpośrednim dowodem na zainteresowanie organów ścigania wykorzystywaniem metod białego wywiadu w Internecie jest ogłoszenie przez Federalne Biuro Śledcze (FBI) „zapytania o informację" (*Request for Information*) dotyczącego możliwości stworzenia i dostarczenia platformy informatycznej służącej do wyszukiwania, mapowania i analizy informacji ze źródeł otwartych[21]. Dokument omawiający szczegóły takiego narzędzia (które miałoby stanowić wsparcie dla FBI SIOC – Strategic Information and Operations Center) wymienia zastosowania operacyjne i analityczne

[17] Szczegółowy opis badań wraz z analizą: W Filipkowski, *Wykorzystanie otwartych źródeł informacji. Wyniki badań ankietowych*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 135–162.

[18] B. Święczkowski, *Wykorzystanie tzw. białego wywiadu w działalności analityczno-informacyjnej Agencji Bezpieczeństwa Wewnętrznego*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 174.

[19] PRIME: Preventing, Interdicting and Mitigating Extremism: Defending Against Lone Actor Extremist Events. EC Grant Agreement n. 608354 (PRIME) FP7-SEC-2013-1.

[20] Badania przeprowadzone w dniach 27 kwietnia – 1 maja 2015 r. w SVP National Police Academy, Hajdarabad, Indie, w ramach szkolenia Mid-Career Training Programme Phase-IV „Strategy, Innovation and Management".

[21] https://www.fbo.gov/index?s=opportunity&mode=form&id=c65777356334dab8685984fa74bfd636&tab=core&_cview=1 (dostęp 10.01.2015 r.).

wymagane przez SIOC, wyliczając *explicite* monitorowanie środowisk Twitter, Facebook i MySpace[22].

Biorąc pod uwagę powyższe obserwacje, trzeba się zastanowić nad umiejscowieniem białego wywiadu w nauce kryminalistyki. Ponieważ ze względu na wykształcenie i doświadczenie zawodowe adresatów „Problemów Współczesnej Kryminalistyki" nie ma potrzeby przeprowadzenia wykładu z zakresu dziedzin i funkcji tej dyscypliny naukowej, wystarczy powiedzieć, że w aktualnej polskiej rzeczywistości prawnej wykorzystanie przez Policję i inne instytucje odpowiedzialne za zapobieganie przestępczości i jej zwalczanie metod i technik białego wywiadu to domena taktyki kryminalistycznej, realizującej jej funkcję rozpoznawczą. Warto podkreślić, że taka konstatacja znajduje poparcie środowiska naukowego (identyczna obserwacja P. Chlebowicza: „biały wywiad należałoby lokować w obszarze taktyki kryminalistycznej, przy czym jego zastosowanie odnosiłoby się przede wszystkim do realizacji funkcji rozpoznawczej"[23]). Jak pisze E. Gruza, funkcja rozpoznawcza kryminalistyki „realizowana jest przez opracowywanie metod i środków służących do uzyskiwania możliwie największej liczby informacji o miejscach, przedmiotach, osobach, taktyce aktualnych i przyszłych działań kryminalistycznych"[24]. Kluczowe jest tu pojęcie informacji, której rola w dziedzinie całej kryminalistyki – jak zauważa T. Hanausek – jest ogromna; autor ten podkreśla również stymulacyjną funkcję informacji, pisząc, że „każda informacja nie tylko przenosi cechy poznawanego przedmiotu do świadomości poznającego podmiotu, ale z reguły jest także stymulatorem działań podejmowanych przez ten podmiot w związku z jej treścią. W takich przypadkach informacja staje się także czynnikiem kształtującym treści, zakres oraz kierunek tych działań"[25]. Te obserwacje okażą się istotne w dalszej części niniejszego wywodu, przy prezentacji zakresu możliwości wykorzystania otwartych źródeł informacji – zarówno przez organa ścigania, jak i przestępców i terrorystów.

Ponieważ pojawiają się niekiedy zastrzeżenia, czy praca na otwartych źródłach informacji nie powinna być uznawana za jedną z form czynności operacyjno-rozpoznawczych, warto zwrócić uwagę na stanowisko wyrażone przez J.D. Pogorzelskiego, który w swojej analizie białego wywiadu w pracy prokuratora stwierdza, że „pozyskiwanie i analiza informacji z otwartych źródeł nie stanowią czynności operacyjno-rozpoznawczych"[26]. Pewne wątpliwości w odniesieniu do uznania metod białego wywiadu w pracy Policji za czynności operacyjno-rozpoznawcze ma W. Mą-

[22] https://www.fbo.gov/utils/view?id=7f9abf0ff0fdba171d1130ddf412aea3 (dostęp 10.01.2015 r.).

[23] P. Chlebowicz, *Biały wywiad z perspektywy kryminalistyki*, op. cit., s. 61.

[24] E. Gruza, *Historia, przedmiot i zadania kryminalistyki*, w: E. Gruza, M. Goc, J. Moszczyński (red.), *Kryminalistyka – czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 22.

[25] T. Hanausek, *Zarys taktyki kryminalistycznej*, Dom Wydawniczy ABC, Warszawa 1994, s. 71.

[26] J.D. Pogorzelski, *Wykorzystanie otwartych źródeł informacji w pracy prokuratora*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 186.

drzejowski, który podaje, że o ewentualnym uznaniu pracy na źródłach otwartych za czynności operacyjno-rozpoznawcze można byłoby mówić w kontekście form pozyskiwania tychże danych; zwraca uwagę na to, że „podstawowe znaczenie ma w tym wypadku kwestia jawności działań policyjnych”[27] – należy zatem rozumieć, że informacyjna czy rozpoznawcza rola białego wywiadu niekoniecznie musi przekładać się na „niejawność” czynności, a dopiero pewne szczególne warunki prowadzenia pracy na źródłach otwartych (np. kamuflowana penetracja, zastosowanie podstępu, użycie specjalistycznego oprogramowania) mogłyby sprawić, że konkretne formy wykorzystania źródeł OSInt zostałyby uznane za czynności operacyjno-rozpoznawcze. Również z perspektywy Agencji Bezpieczeństwa Wewnętrznego problematyka prowadzenia działań w oparciu o informacje ze źródeł otwartych może być postrzegana nie jako czynność operacyjno-rozpoznawcza, ale analityczno-informacyjna[28].

Powyższe omówienie posłużyć ma jako przyczynek do rozważań na temat możliwości wykorzystania otwartych źródeł informacji pochodzących z Internetu i powiązanych z siecią nowoczesnych technologii przez organa ścigania i służby wywiadowcze oraz przez sprawców przestępstw i zamachów terrorystycznych. W mojej opinii Internet staje się „polem bitwy”[29], na którym obie strony konfliktu walczą o dominację. Odchodzę przy tym od tradycyjnego pojmowania cyberprzestępczości (która w powszechnym odbiorze dotyczy zdarzeń „dziejących się” w świecie cyfrowym) na rzecz podejścia, w którym Internet jest narzędziem dokonywania przestępstw, do jakich dochodzi w świecie rzeczywistym. Ze względu na zobrazowane wyżej trendy w rozwoju samej sieci Internetu, stały wzrost liczby użytkowników, a także pojawiających się regularnie nowych aplikacji i narzędzi, będziemy bowiem zauważać dalszy wzrost skali przestępczości, w której nowe technologie wykorzystywane będą nie tylko do dokonywania czynów zabronionych w świecie wirtualnym, ale także – a z czasem: przede wszystkim – w świecie realnym. Wynika to z kilku przyczyn[30]:

1. nowoczesne technologie i Internet umożliwiają użytkownikom bezprecedensowo łatwy i szeroki dostęp do informacji i kontaktów;
2. narzędzia informatyczne dostępnie obecnie w obrocie internetowym są łatwe w użyciu, a ich wykorzystanie nie wymaga od użytkowników posiadania specjalistycznej wiedzy fachowej (lub daje możliwość skorzystania z pomocy łatwych do zrozumienia instrukcji – w tym poradników wideo pokazujących algorytmy postępowania);
3. zarówno sam Internet, jak i powiązane z nim technologie są łatwo dostępne, a jednocześnie bardzo tanie (niekiedy darmowe);

[27] W. Mądrzejowski, *Biały wywiad w Policji*, w: W. Filipkowski, W. Mądrzejowski (red.), op. cit., s. 126.

[28] Por. B. Święczkowski, op. cit., s. 165–167.

[29] K. Gradoń, *Crime science and the battlefield of the Internet. Securing the analog world from the digital crime*, „IEEE Security & Privacy Magazine”, 2013, Vol. 11 Issue No. 5 (September-October) 2013, s. 93–96.

[30] K. Gradoń, *Internet Crime*, w: M.E. Beare (red.), *Encyclopedia of Transnational Crime & Justice*, SAGE, Thousand Oaks 2012, s. 212.

4. narzędziami tego rodzaju można się posługiwać (przy minimum wiedzy fachowej) z zachowaniem relatywnie wysokiego poziomu anonimowości.

Najważniejszą jednak przyczyną, dla której twierdzę, że obserwując fenomen z perspektywy analizy strategicznej, można zakładać z ogromną dozą pewności, iż w nieodległej przyszłości zaobserwujemy przeniesienie się zauważalnej części działalności przestępczej i terrorystycznej do Internetu, są przemiany pokoleniowe. Osoby urodzone po 1980 roku nazywane były już kilka lat temu „generacją sieci”[31], jednak w owym czasie odnoszono się przede wszystkim do działalności społecznej, ekonomicznej czy kulturalnej, która w coraz większym stopniu przenosiła się do przestrzeni wirtualnej. Moim zdaniem te same problemy muszą przekładać się na przestępczość, zatem z im młodszym pokoleniem sprawców (bądź: potencjalnych sprawców) będziemy mieć do czynienia, tym większe prawdopodobieństwo tego, że Internet będzie głównym i oczywistym elementem ich „środowiska naturalnego”[32].

Celem niniejszego opracowania nie jest diagnoza socjodemograficzna czy pedagogiczna, jednak jeśli się przyjmie założenie, że obecnie Internet jest jednym z najważniejszych lub głównym miejscem zdobywania informacji[33], to oczywiste się staje, że już niedługo będziemy mieć do czynienia z pokoleniem przyzwyczajonym od najwcześniejszych lat życia (i edukacji) do intensywnego korzystania z mediów elektronicznych oraz zdobywania większości swej wiedzy i informacji w sieci. Przedstawiciele tego pokolenia, którzy na pewnym etapie rozwoju zdecydują się na zaangażowanie w działalność przestępczą, będą traktować Internet jako narzucające się narzędzie „pierwszego wyboru”, służące początkowo do zdobywania know-how, a w dalszej kolejności do przygotowania i przeprowadzenia zamierzonego i zaplanowanego przestępstwa[34]. Wynika to wprost z wymienionych wyżej przyczyn (dostęp do informacji i kontaktów, łatwość wykorzystania narzędzi, bardzo wysoka dostępność, niskie koszty, relatywnie wysoka anonimowość) i sprawia, że Internet staje się dla aktywnych bądź potencjalnych sprawców ekwiwalentem „wielofunkcyjnego noża”, łatwego w obsłudze i pomocnego w osiąganiu szerokiego spektrum zakładanych celów.

Już na początku XXI wieku zauważono, że „cyberprzestrzeń pozwala obecnie na wiele takich samych działań jak główna ulica miasta. Możemy angażować się tam w cyberzakupy, cyberrandki i cyberkształcenie. Jednakże tak jak i na głównej ulicy miasta mamy tam również do czynienia z mroczną stroną: cyberkradzieżami, cyberoszustwami i cyberniszczeniem”[35]. Przez kolejne kilkanaście lat problem ten

[31] *The net generation, unplugged*, „The Economist”, 4 marca 2010 r., http://www.economist.com/node/15582279 (dostęp: 6.07.2014).
[32] K. Gradoń, *Internet as a new criminal battleground? An essay on the future trends in crime*, „Przegląd Naukowy Disputatio” 2011, t. XII, s. 153.
[33] Por. np. M. Szpunar, *Internet – medium informacji versus dezinformacji*, „E-mentor. Dwumiesięcznik Szkoły Głównej Handlowej w Warszawie” 2007, nr 2, s. 46–51.
[34] K. Gradoń, *Internet as a new criminal battleground?...*, op. cit., s. 153.
[35] D.C. Kennedy, *In search of a balance between police power and privacy in the Cybercrime Treaty*, „Richmond Journal of Law and Technology” 2002, No. 9, s. 58.

w sposób wyraźny zyskał na znaczeniu i intensywności, a możliwości, jakie daje sprawcom przestępstw współczesna technologia, są nieporównywalnie większe od potencjału oferowanego przez sieć nieco ponad dekadę temu. Wiąże się to nie tylko z samym rozwojem techniki, ale także z pojawieniem się w latach 2001–2002 nowego fenomenu znanego pod nazwą „Web 2.0" (sieć drugiej generacji) – czyli platform i serwisów, których zawartość tworzona jest przez samych użytkowników (a nie jedynie transmitowana do nich przez jednostki zewnętrzne: administratorów stron czy redakcje mediów elektronicznych)[36]. Właśnie takie serwisy – czyli przede wszystkim media społecznościowe – stanowią obecnie główne otwarte źródło informacji.

Nick Ross, współzałożyciel i fundator Jill Dando Institute of Crime Science w University College London, jednostki przekładającej wyniki multidyscyplinarnych i empirycznych badań naukowych na praktyczne strategie kontroli i zwalczania przestępczości (nowa dyscyplina pod nazwą *Crime Science*[37]), odnosząc się do przyszłych trendów w przestępczości, pisze w alarmistycznym tonie: „Internet to miejsce, w którym w przyszłości przeprowadzane będą jedne z najstraszniejszych zbrodni. Jeśli trend (który obserwujemy) będzie dalej iść w tym kierunku, cyberprzestępczość prawdopodobnie stanie się jednym z największych zagrożeń, pomijając zarazy i wojnę atomową"[38]. Taka opinia może wydawać się nieco przesadzona, jednak jak postaram się poniżej wykazać, ryzyko zdominowania przestępczego krajobrazu przez zdarzenia powiązane w pewnym stopniu z cyberprzestrzenią i nowymi technologiami jest wysokie.

Jednym z pierwszych powszechnie znanych przykładów możliwości, jakie dają potencjalnym przestępcom pochodzące z Internetu dane jawnoźródłowe, było wielokrotne zabójstwo, którego dopuścili się w 1999 roku w liceum Columbine High School w stanie Kolorado dwaj nastolatkowie – Eric Harris i Dylan Klebold. Rozwój Internetu był w tamtych czasach na nieporównywalnie niższym – w stosunku do dzisiejszego – poziomie, jednak obaj sprawcy korzystali z dostępnych im narzędzi, zdobywając dzięki nim instrukcje budowy improwizowanych materiałów wybuchowych[39] (dostępna w sieci w formie edytowalnego pliku tekstowego tzw. „Anarchistyczna książka kucharska" i podręcznik armii amerykańskiej *TM 31-210 Improvised Munitions Handbook*), ucząc się taktyki działania oddziałów specjalnych i metod komunikacji w sytuacji frontowej (również dostępny w sieci – w formie pliku tekstowego – podręcznik Armii Stanów Zjednoczonych *US Marine Corps Jungle & Urban Warfare Manual*), jak również zapoznając się ze schematami działania służb policyjnych, ratowniczych i medycznych (oryginalnym zamiarem sprawców

[36] Por. np. T. O'Reilly, *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, 09.30.2005, http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (dostęp 8.12.2014 r.).

[37] por. http://www.ucl.ac.uk/scs.

[38] N. Ross, *Crime – How to Solve It and Why So Much of What We're Told is Wrong*, Biteback Publishing, London 2013, s. 295–296.

[39] K. Gradoń, *Zabójstwo wielokrotne. Profilowanie kryminalne*, Lex Wolters Kluwer, Warszawa 2010, s. 29–35.

było spowodowanie w szkole potężnej eksplozji obliczonej na zabicie kilkuset ofiar, egzekucja osób, którym udałoby się wydostać z ruin, i wreszcie samobójstwo. Kilkadziesiąt minut później miało dojść do detonacji bomb ukrytych w samochodach zaparkowanych przy szkole, co w zamiarze zamachowców spowodowałoby śmierć kolejnych osób, które pojawiłyby się na miejscu tragedii. Plan nie powiódł się ze względu na usterki zapalników czasowych w ładunkach wybuchowych, wobec czego sprawcy wkroczyli do budynku szkoły i otworzyli ogień do uczniów i nauczycieli. Charakterystycznym elementem działania przestępców było w tym przypadku ogłaszanie w Internecie informacji wyprzedzających na temat planowanego zamachu.

Podobny schemat działania[40], rozwinięty tylko o możliwości, jakie daje Web 2.0 (czyli przede wszystkim portale społecznościowe), możemy zaobserwować również w innych atakach tego rodzaju – np. zabójstwie dokonanym w 2006 r. przez Kimveera Gilla w Dawson College w Montrealu, ataku Seung-Hui Cho na Politechnikę Stanu Virginia (2007 rok, 32 ofiary śmiertelne) czy masakrze w fińskim liceum Jokela (atak Pekki-Erica Auvinena w 2007 roku, 10 ofiar śmiertelnych). Sprawcy tych zbrodni nie tylko ogłaszali swoje plany w Internecie, ale także radykalizowali się i szkolili za pomocą dostępnych tam źródeł.

Również sprawca ataku w Oslo i na wyspie Utoya, Anders Breivik, był aktywnym użytkownikiem Internetu, a przygotowana przez niego i dokonana w 2011 roku zbrodnia została w znacznym stopniu opracowana w szczegółach właśnie dzięki otwartym źródłom informacji. Breivik nie tylko radykalizował się za pośrednictwem sieci, ale również planował zamach, uczył się technik działania i zdobywał niezbędne mu umiejętności przy użyciu metod, które moglibyśmy nazwać białym wywiadem[41].

Problem radykalizacji za pomocą Internetu traktowanego jako otwarte źródło informacji to bardzo poważny i skrajnie niebezpieczny fenomen, szczególnie istotny w ostatnich latach, kiedy to regularnie stykamy się z doniesieniami na temat szerzenia ideologii ekstremistycznej właśnie za pośrednictwem nowoczesnych technologii. Niektórzy autorzy posuwają się nawet do określania Internetu mianem „bodźca gniewu" (*rage enabler*)[42] dla podatnych na ekstremistyczne wpływy jednostek. Problematyka „radykalizacji on-line" jest zbyt szeroka, by ująć ją w niniejszym artykule, jednak warto wymienić przynajmniej publikatory takie jak wydawany przez organizację terrorystyczną Al-Kaida w formie elektronicznej magazyn „Inspire", którego głównym celem jest szerzenie ideologii islamskiego dżihadu, a także zachęcanie i szkolenie potencjalnych zamachowców oraz legitymizacja ataków[43]. Fenomen ten nabiera szczególnego znaczenia w obliczu zagrożenia kampanią salafickiej organizacji terrorystycznej Państwo Islamskie (ISIS), która wykorzystuje Internet i media

[40] Tamże.

[41] R. Pantucci, *What have we learned about lone wolves from Anders Behring Breivik?*, „Perspectives on Terrorism" 2011, Vol. 5, No. 5–6, s. 27–41.

[42] B. Forst, *Terrorism, Crime and Public Policy*, Cambridge University Press, New York, 2009, s. 190.

[43] http://www.foxnews.com/world/2010/07/01/make-bomb-kitchen-mom-featured-al-qaedas-st-english-magazine/ (dostęp 10.02.2015 r.).

społecznościowe jako jedno ze swoich podstawowych narzędzi zarówno białego wywiadu, jak i propagandy[44]. Kompleksową analizę tej formy wykorzystania Internetu przez terrorystów zawiera raport korporacji RAND pt. *Radicalisation in the Digital Era*[45].

Jak ustalono wcześniej, z perspektywy instytucji zaangażowanych w zwalczanie przestępczości kryminalnej i samych przestępców otwarte i powszechnie dostępne dane znajdujące się w Internecie (ze szczególnym uwzględnieniem sieci i portali społecznościowych) stanowią niezwykle wartościowe źródło informacji. W tym miejscu należy się więc skoncentrować na opisie wybranych możliwości, jakie oferują pod tym względem nowoczesne technologie. Starając się zachować przejrzystość wywodu, zaprezentujemy wyliczone poniżej narzędzia i techniki z punktu widzenia potencjału ich wykorzystania przez przestępców. Przyczyną takiego ujęcia tematu jest fakt, że populacja osób prywatnych, które nie są zaangażowane w działalność przestępczą (ewentualnych ofiar przestępstw) i do których danych osobowych sprawcy mają obecnie nieograniczony dostęp, jest znacząco większa niż populacja sprawców. Kieruję się zatem postulatem zasygnalizowania zagrożeń i wpłynięcia w ten sposób na zwiększenie ich świadomości, a jednocześnie realizację założeń prewencyjnej funkcji kryminalistyki, co w konsekwencji powinno się przekładać na podniesienie bezpieczeństwa. Oczywiście te same metody i techniki uzyskiwania i wykorzystywania danych pochodzących ze źródeł otwartych mogą być stosowane na poziomie analitycznym i operacyjnym przez instytucje i służby odpowiedzialne za zwalczanie przestępczości i jej zapobieganie.

Dostępne w niekontrolowany sposób dane dotyczące osób i miejsc mogą być wykorzystywane przez sprawców do typowania, wyboru i monitoringu celów ataku. Pomagają m.in. w ustaleniu, czy cel (ofiara) należy do kategorii niskiego, czy wysokiego ryzyka. Opierając się na dostępnych danych, sprawca może analizować wiek, zawód, styl życia, budowę ciała, kondycję fizyczną, możliwości samoobrony i okolicę, w której ofiara mieszka lub przebywa. W związku z tym wyróżnia się tzw. ofiary wysokiego ryzyka, przebywające w okolicach, w których są bardziej bezbronne (np. pętle autobusowe, odosobnione miejsca, parki, lasy, tereny otwarte lub okolice o dużym nasyceniu prostytucją), i sprawiające wrażenie łatwiejszego celu ataku (np. osoby bardzo młode lub w podeszłym wieku), oraz tzw. ofiary niskiego ryzyka, których zawód i styl życia sprawiają, że najczęściej nie stają się ofiarami przestępstw z użyciem przemocy (m.in. ze względu na okolice, w których mieszkają, pracują lub spędzają wolny czas)[46]. Na tej samej zasadzie sprawca może oceniać „opłacalność" ataku na konkretną osobę lub miejsce – bazując na źródłach otwartych, może

[44] http://www.geopoliticalmonitor.com/islamic-state-online-jihadist-propaganda-2-0/ (dostęp 8.03.2015 r.).

[45] I. von Behr, A. Reding, C. Edwards, L. Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, RAND Corporation, Santa Monica, CA, 2013.

[46] Jest to bezpośrednie przełożenie metod wykorzystywanych w profilowaniu kryminalnym. Por. K. Gradoń, *Zabójstwo wielokrotne*..., op. cit., s. 169.

rozpoznać stopień zamożności ofiary albo ocenić wartość konkretnych składników jej majątku.

Już podstawowe wyszukiwania w sieci pozwalają przeciętnemu użytkownikowi Internetu (a więc również sprawcom przestępstw) na poznanie danych osobowych ofiary. Umiejętność kojarzenia zespołów danych pochodzących z różnych stron i portali internetowych umożliwia stworzenie bardzo kompletnego dossier konkretnej osoby. Generalną zasadą jest, że intensywność aktywności sieciowej rozumianej jako udzielanie się czy obecność w różnych serwisach, portalach, forach dyskusyjnych i platformach społecznościowych jest wprost proporcjonalna do stopnia niekontrolowanego wycieku danych i potencjalnego zagrożenia dla osoby, której taka działalność jest udziałem. Brzmi to jak truizm, jednak większość użytkowników Internetu nie zdaje sobie z tego sprawy lub nie dopuszcza do świadomości ewentualnego ryzyka, na jakie się narażają. Przykładowo w ramach eksperymentów związanych z prowadzonymi badaniami przeprowadziłem testy penetracyjne dotyczące kilku osób (za ich zgodą), co do których wiedziałem, że są regularnymi użytkownikami Internetu. Dla celów badawczych celowo wytypowałem osoby, które nie używają serwisów mikroblogowych (Twitter) ani nie prowadzą blogów (natura tych platform sprawia, że autorzy publikowanych tam wpisów czy komentarzy częściej dzielą się z czytelnikami swoimi informacjami osobistymi). Skojarzenie danych pochodzących z kilku stron i portali społecznościowych (popularne Facebook i LinkedIn, nieco mniej powszechne Goldenline, ciesząca się niegdyś dużym uznaniem Nasza-Klasa, a także proste wyszukiwania za pomocą wyszukiwarki Google) pozwoliły mi na zebranie kompletów danych, wśród których znajdowały się imiona i nazwiska (w tym nazwiska panieńskie), daty urodzenia, aktualne i poprzednie adresy, kompletne informacje o wykształceniu na wszystkich szczeblach edukacji, adresy e-mail, numery telefonów prywatnych i służbowych, imiona i nazwiska osób bliskich (w tym nazwiska panieńskie), szczegółowe informacje o dzieciach, dane zawodowe dotyczące aktualnych i poprzednich miejsc zatrudnienia, informacje o hobby, zainteresowaniach, sposobach i miejscach spędzania wolnego czasu, regularnym planie dnia, informacje pozwalające na postawienie realistycznych założeń na temat statusu majątkowego oraz obfite zbiory fotografii „oficjalnych" i prywatnych, w tym fotografie spełniające warunki przewidziane dla zdjęć biometrycznych (w czego potwierdzeniu pomaga np. dostępne on-line narzędzie Photo Tool[47] wykorzystywane przez Departament Stanu USA przy internetowym systemie wniosków wizowych). Za zgodą dwóch wyselekcjonowanych osób przeprowadziłem na podstawie zebranych danych dalsze testy bezpieczeństwa dotyczące możliwości złamania zabezpieczeń należącej do nich poczty elektronicznej. Większość dostawców serwisów poczty e-mail oferuje swoim użytkownikom opcje pytań zabezpieczających wykorzystywanych do odzyskiwania haseł w przypadku ich zapomnienia. Najczęściej pytania zabezpieczające dostępne są z rozwijanego menu i z reguły są one zaproponowane użytkownikowi (większość serwisów pozwala co prawda na tworzenie własnych, jednak przeważająca grupa

[47] http://travel.state.gov/content/visas/english/general/photos.html (dostęp 15.03.2015 r.).

osób wybiera sugerowane pytania z przedstawionej im listy[48]). „Złamanie" pytań zabezpieczających ograniczyło się w obu przypadkach do udzielenia poprawnej odpowiedzi na te pytania, te zaś można było błyskawicznie znaleźć w wymienionych wyżej serwisach społecznościowych (pytania w rodzaju: „nazwisko panieńskie matki", „imię psa", „patron pierwszej szkoły", „nazwisko pierwszego nauczyciela"). Reset hasła do skrzynki e-mail pozwalał na zapoznanie się z jej zawartością, w tym odnalezienie elektronicznych wyciągów bankowych z pełnymi informacjami o rachunku, jak również faktur zawierających numery NIP i dane innych kont bankowych powiązanych z użytkownikiem.

Potencjał ustalania danych osobowych w Internecie jest ogromny, a wielu użytkowników, w całkowitej nieświadomości zagrożenia, udostępnia jeszcze bardziej precyzyjnie je identyfikujące materiały. Przykładowo wspomniany wyżej fotograficzny serwis społecznościowy Instagram umożliwia swoim użytkownikom umieszczanie zdjęć, które opisywane są przy użyciu słów kluczowych (tzw. hashtagów). Niektórzy użytkownicy zamieszczają w tym serwisie fotografie swoich dowodów osobistych, praw jazdy, paszportów, kart płatniczych, mandatów karnych (!), aktów notarialnych, rachunków itp. Ponieważ zamieszczone tam zdjęcia opisywane są słowami kluczowymi, ich znalezienie nie przedstawia większego problemu. Fenomen ten opisany został w grudniu 2013 r. przez serwis Niebezpiecznik.pl, który zwrócił uwagę na możliwość wykorzystania innej aplikacji (zwanej wówczas Statigram) do przeszukiwania zasobów Instagramu po słowach kluczowych[49]. Obecnie Statigram został zastąpiony nowocześniejszą wyszukiwarką Iconsquare[50], dzięki której można prowadzić efektywne wyszukiwania hashtagów Instagramu. Proste ćwiczenie (sprowadzające się wyłącznie do wymyślania „kreatywnych" słów kluczowych powiązanych z danymi osobowymi – w języku polskim i angielskim) umożliwia błyskawiczny dostęp do znacznej liczby dokumentów zawierających dane wrażliwe (niejednokrotnie ich komplety; szczególnie kuriozalny przykład to przypadek osoby, która zamieściła w serwisie Instagram fotografie awersów i rewersów swojego dowodu osobistego, prawa jazdy i karty debetowej).

Tworzenie profilu czy dossier ofiary przy użyciu otwartych źródeł informacji pozwalać może na dotarcie do informacji wrażliwych, w tym danych medycznych i szczegółów związanych ze stanem zdrowia i kondycją fizyczną. Wielu użytkowników Internetu poszukuje wstępnych porad medycznych w przestrzeni wirtualnej, a pięć z dwudziestu największych grup dyskusyjnych poświęconych takim poradom zrzesza (w Polsce) od 1 do 2,2 miliona użytkowników. Łącznie ze wszystkich grup dyskusyjnych korzysta w naszym kraju ponad 7 milionów unikalnych użytkowników[51]. Natura rozmów prowadzonych na tego typu forach i w grupach dyskusyj-

[48] http://time.com/3892793/security-questions-answer/ (dostęp 3.06.2015 r.).

[49] http://niebezpiecznik.pl/post/instagram-pelen-zdjec-dowodow-praw-jazdy-i-kart-platniczych-polakow/ (dostęp 7.05.2014 r.).

[50] http://iconosquare.com.

[51] Raport *Pacjenci w sieci* przygotowany przez Procontent Communication, Warszawa, styczeń 2012. Dostęp: http://pliki.gemius.pl/Raporty/2012/Raport_Pacjenci_w_sieci_20121.pdf.

nych sprawia, że większość uczestników posługuje się tam pseudonimami (nickami) i teoretycznie unika ujawniania swojej tożsamości. Proste przeszukanie podobnych list dyskusyjnych wskazuje jednak na to, że stosunkowo częstym zjawiskiem jest rejestrowanie się użytkowników przy użyciu adresu e-mail (niekiedy podawany przez uczestników w celu kontynuacji dyskusji na konkretny temat poza forum), ten zaś z kolei pozwala na znalezienie innych miejsc w sieci, w których dana osoba rejestrowała się przy użyciu tego samego adresu, ale już pod swoim prawdziwym imieniem i nazwiskiem. Testowy przegląd kilku medycznych grup dyskusyjnych umożliwił mi znalezienie w specjalistycznych wątkach znacznie bardziej szczegółowych informacji zdrowotnych – w tym skanów z epikryz szpitalnych, kopii wyników analiz lekarskich i badań obrazowych – w tych przypadkach udostępniający dokumenty (najprawdopodobniej ich właściciele) nie zadbali o usunięcie wyjątkowo wrażliwych danych (zarówno identyfikacyjnych, jak i ściśle osobistych, dotyczących stanu zdrowia).

Wyszukiwanie po pseudonimach/nickach, adresach e-mail lub adresach IP umożliwia osobom ukierunkowanym na zbieranie danych ze źródeł otwartych dotarcie do specyficznych informacji, które niejednokrotnie mogą być uznane za dane wrażliwe (w tym kompromitujące lub wstydliwe). Jeżeli osoba używa charakterystycznego pseudonimu (do którego jest przyzwyczajona, przywiązana), to jest możliwe, że korzysta z niego w różnych sytuacjach, tj. np. w kilku niepowiązanych ze sobą miejscach sieci. Podobny mechanizm dotyczy wykorzystywania adresów poczty elektronicznej. Takie postępowanie jest naturalną i pragmatyczną, ukierunkowaną na własną wygodę postawą, właściwą większości ludzi[52]. Znając charakterystyczny nick czy adres e-mail interesującej nas osoby, możemy spróbować znaleźć ślady jej działania na różnych stronach w Internecie, docierając niekiedy do treści, których taka osoba wolałaby nie podpisywać własnym nazwiskiem, w trosce o swoje dobre imię lub pod wpływem innych przyczyn motywacyjnych. Rzecz jasna, nie można być wówczas pewnym tożsamości autora takich treści (bazując na samym pseudonimie), jednak ocena psycholingwistyczna publikowanych treści (tj. „szczegółowa analiza pisemnej (…) wypowiedzi ich autora, zarówno od strony formy wypowiedzi, sposobu (…) pisania, jak i zawartości – treści, składni gramatycznej, częstotliwości używania określonych słów, stosowanych zwrotów i idiomów, popełnionych błędów językowych i ortograficznych”[53]) może w znacznym stopniu uprawdopodobnić hipotezę dotyczącą osoby autora i rozszerzyć naszą wiedzę na jego temat o nietypowe czy trudne do zdobycia w inny sposób informacje. Warto zauważyć, że w ten sam sposób możemy dotrzeć do profilu interesującej nas osoby w serwisach dotyczących np. recenzji wystaw, koncertów, przedstawień, filmów, restauracji czy hoteli (dzięki czemu można rozbudować „dossier” o informacje o gustach czy możliwościach finansowych i sposobach spędzania wolnego czasu) oraz do profili w serwisach aukcyjnych (takich jak eBay czy Allegro), co może pozwolić na prześledzenie historii

[52] Por. koncepcja „rachunku szczęśliwości” (*Felicific Calculus*) sformułowana przez Jeremy’ego Benthama.

[53] E. Gruza, *Wybrane działania rozpoznawczo-wykrywcze*, w: E. Gruza, M. Goc, J. Moszczyński (red.), op. cit., s. 56.

zakupów i sprzedaży i dotarcie do bardzo specyficznych szczegółów składających się na profil socjoekonomiczny danego człowieka[54].

Kolejnym problemem, który wiąże się z tematyką białego wywiadu w Internecie, jest kwestia uzyskiwania danych o geolokalizacji użytkownika. Poza rozwiązaniami niemieszczącymi się w pojęciu źródeł otwartych (zazwyczaj też nielegalnymi i często wymagającymi specjalnych umiejętności od użytkownika, czyli np. zarażenia telefonu komórkowego ofiary za pomocą złośliwego oprogramowania), aktualne rozwiązania oferowane przez Internet i powiązane z nim nowoczesne technologie pozwalają na posłużenie się oficjalnie dostępnymi i jawnymi narzędziami do zdobycia precyzyjnych informacji na temat fizycznej przestrzeni, w której znajduje się cel ataku (osoba lub miejsce).

Najprostszą metodą jest odczytanie danych geolokalizacyjnych miejsca wykonania fotografii umieszczonej przez autora w Internecie. Jeżeli zdjęcie zostało zrobione przy użyciu aparatu cyfrowego mającego na wyposażeniu włączony moduł GPS (obecnie coraz więcej zdjęć jest wykonywanych nie tradycyjnym aparatem fotograficznym, ale cyfrową kamerą umieszczoną w telefonie typu smartphone, zawierającym zazwyczaj funkcję GPS), to w pliku metadanych zdjęcia (EXIF) znajdą się dokładne współrzędne miejsca wykonania zdjęcia oraz informacje o dacie i godzinie wykonania fotografii. Można dzięki temu potwierdzić obecność osoby w danym miejscu i mieć pewność co do czasu, w jakim się tam znajdowała. Daje to duże możliwości także organom ścigania, łatwiej jest im bowiem dzięki temu wytypować potencjalne miejsca, w których może przebywać poszukiwana przez nie osoba[55].

Dane fotograficzne dostępne w Internecie (dotyczy to zarówno metadanych, jak i po prostu obiektów uwidocznionych na zdjęciach) mogą pomóc nawet w prowadzeniu operacji militarnych, czego przykładem jest precyzyjny atak lotnictwa amerykańskiego na siedzibę organizacji terrorystycznej Państwo Islamskie (ISIS) 3 czerwca 2015 roku. Atak został przygotowany dzięki prywatnym fotografiom terrorysty z ISIS; prezentował na nich samego siebie przed budynkiem, w którym mieściła się jednostka dowodzenia ISIS; fotografie te umieszczone były w jednym z serwisów społecznościowych[56]. Zbliżona sytuacja z lipca 2014 roku była nieformalnym potwierdzeniem obecności wojsk armii rosyjskiej na terytorium Ukrainy: rosyjski żołnierz wykonał swoje autoportrety i umieścił je w serwisie Instagram – metadane zdjęcia dotyczące lokalizacji geograficznej wskazywały, że w momencie zrobienia zdjęcia musiał znajdować się na Ukrainie[57]. Podobny potencjał mają metadane

[54] Badanie danych z serwisów aukcyjnych, wykraczające poza tematykę białego wywiadu, a związane raczej z pracą operacyjną, pracą dochodzeniowo-śledczą i informatyką śledczą, jest problemem zasługującym na oddzielną publikację. Por. np. „eBay Toolbar in Forensic Investigations" dostępne: http://computer-forensics.7safe.com/ebay-toolbar-in-forensic-investigations/ (dostęp: 14.12.2014 r.).

[55] Por. np. http://exifdangers.blogspot.com/ (dostęp 11.06.2015 r.).

[56] http://www.militarytimes.com/story/military/tech/2015/06/04/air-force-isis-social-media-target/28473723/ (dostęp 5.06.2015 r.).

[57] http://www.businessinsider.com/russian-soldier-ukraine-2014-7 (dostęp 10.08.2014 r.).

w wiadomościach publikowanych w serwisie mikroblogowym Twitter, powiązanych z usługą geolokalizacyjną oferowaną przez moduł Foursquare, którego użytkownicy mogą oznaczać miejsce pobytu w chwili zamieszczenia wiadomości na swoim profilu w Twitterze. Świadczy to wówczas o ich fizycznej obecności w danym miejscu, jak również o tym, że nie znajdują się np. w swoim mieszkaniu (co może pomóc przestępcom w oszacowaniu czasu, jaki mają na dokonanie włamania)[58].

Sprawcy przestępstw mogą korzystać z dostępnych im narzędzi przy przygotowaniu i planowaniu ataków. Prostą metodą rekonesansu jest użycie internetowych serwisów mapowych. W Internecie dostępne są zarówno profesjonalne ortofotomapy, jak i szczegółowe mapy topograficzne, drogowe i satelitarne. Najpopularniejsza aktualnie platforma Google Maps oferuje mapy satelitarne wysokiej jakości i dużej wiarygodności, zawierające w niektórych częściach świata renderowanie trójwymiarowe. Ogromną popularnością cieszy się funkcja Google Street View, pozwalająca użytkownikowi na zapoznanie się z fizycznym otoczeniem danego punktu na mapie (znajdującego się w polu widzenia samochodu firmy Google fotografującego okolicę) poprzez panoramiczne widoki z poziomu ulicy. Potencjał przestępczego wykorzystania Google Street View jest bardzo duży. Wymienia się[59] m.in. możliwość obejrzenia celu w ramach przygotowania ataku (np. włamania) i zorientowanie się w otoczeniu fizycznym, pod kątem obecności płotów, żywopłotów, lokalizacji kamer monitoringu, liczbie i położeniu wejść, wytypowanie kryjówek (krzaki, śmietniki), ustalenie umiejscowienia skrzynek z mediami (gaz, woda, elektryczność), określenie marki, modelu i koloru samochodu zaparkowanego na podjeździe przed domem, dokładne zmierzenie odległości od celu ataku do miejsc ewentualnej ucieczki. Wszystko to możliwe jest bez fizycznego zbliżania się do obiektu. Taką strategię zastosowali m.in. terroryści z ugrupowania Lashkar-e-Taiba, którzy dopuścili się ataków w Bombaju w listopadzie 2008 r.[60] Posługując się serwisem Google Maps, uczyli się na pamięć topografii miasta, tak aby po przybyciu na miejsce nie wzbudzać podejrzeń i nie tracić czasu na zapoznawanie się z siatką ulic[61].

Kolejnym przykładem możliwości pobierania informacji geolokalizacyjnych ze źródeł otwartych jest zdobywająca wielką popularność funkcjonalność pozwalająca na przenoszenie informacji ze sportowych zegarków biegowych[62] (Garmin, Suunto) i smartfonów (z aplikacjami sportowymi, np. Endomondo) do serwisów społecznościowych (zarówno tych powszechnych, jak i przeznaczonych specyficznie dla sportowców). Funkcja rejestracji przebiegu trasy biegowej (przy użyciu modułu GPS w zegarku i telefonie) pozwala użytkownikowi na to, by zapis przebytej trasy (oraz

[58] https://cdt.org/blog/over-sharing-and-location-awareness/ (dostęp 10.05.2011 r.).

[59] http://netsecurity.about.com/od/perimetersecurity/a/How-Criminals-Use-Google-Maps-Street-View-To-Case-The-Joint.htm (dostęp 8.06.2014 r.).

[60] K. Gradoń, *Crime science and the battlefield of the Internet*..., op. cit., s. 95.

[61] http://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html?_r=0 (dostęp: 27.12.2014 r.).

[62] Wszystkie obserwacje opisane w tym akapicie poczynione zostały przez autora niniejszego artykułu podczas badań własnych.

informacje o prędkości, tempie, czasie i miejscu rozpoczęcia i zakończenia treningu, a także – w przypadku urządzeń wyposażonych w funkcję pomiaru tętna – średnim i maksymalnym tętnie i spalonych kaloriach) przenieść do komputera domowego i wykorzystać go np. do analizy postępów treningowych. Wiele osób przenosi takie dane również do Internetu – na serwisy w rodzaju Run-Log[63], MapMyRun[64] czy Endomondo[65]. Korzystając z otwartych źródeł informacji (znając nazwisko, adres e-mail lub popularny pseudonim) interesującej nas osoby, możemy w tego rodzaju serwisie odnaleźć jej profil i odczytać wszystkie wymienione wyżej parametry. Dzięki temu dowiedzieć się możemy np. o regularnych trasach biegowych tej osoby, porach dnia rozpoczynania treningu i lokalizacji miejsca startu. Jeżeli mamy do czynienia z osobą uprawiającą sport w sposób regularny, prosta analiza trendów pozwolić nam może na postawienie hipotez odnośnie do tego, czy interesujący nas człowiek będzie danego dnia w określonych godzinach przebywał w konkretnych miejscach. Zazwyczaj jesteśmy też w stanie ocenić, czy punktem startu jest np. dom osoby, czy inne, przypadkowe miejsce. Umożliwia to funkcja satelitarnej warstwy mapy nakładana na elektroniczny zapis przebiegu treningu. Możemy też się domyślać, przez jak długi czas osoba będzie przebywała poza domem i którędy może się przemieszczać. Sprawcy przestępstw mogą dzięki temu wytypować czas ataku na obiekt (np. włamanie do domu pod nieobecność właściciela) lub atak na osobę (napad zaplanowany w miejscu położonym na trasie ofiary, a wygodnym i bezpiecznym dla napastnika). Nawet jeżeli sprawca nie zna tożsamości ofiary, a jedynie planuje włamanie lub napaść w konkretnej okolicy, może sprawdzić w serwisie sportowym, czy w tym rejonie przebywają zarejestrowani na danym portalu biegacze, a następnie podejrzeć ich plany treningowe i miejsca startu. Chociaż większość osób zarejestrowanych na serwisach biegowych nie podaje publicznie swojego nazwiska, tylko figuruje tam pod pseudonimem (nickiem), to biały wywiad umożliwia odnalezienie prawdziwych danych konkretnego człowieka: wiele osób aktywnych w portalach sportowych publikuje swoje fotografie z zawodów, na których zazwyczaj figurują z numerem startowym przypiętym do koszulki. Kolejne otwarte źródło danych (strona internetowa organizatora zawodów) pomaga w powiązaniu numeru startowego z imieniem, nazwiskiem, wiekiem i miastem zamieszkania sportowca. Do tego osoba posiłkująca się metodami białego wywiadu ma dzięki portalom biegowym dostęp do zdjęć interesującego ją człowieka, a niekiedy również danych medycznych lub dotyczących wydolności organizmu (VO2Max, HRMax) i kondycji fizycznej.

Opisane wyżej metody i możliwości wykorzystania Internetu i powiązanych z nim nowoczesnych technologii przez przestępców nie wyczerpują oczywiście tematu białego wywiadu i otwartych źródeł informacji. Ze względu na ograniczoną wielkość artykułu niemożliwe było zasygnalizowanie wszystkich możliwości oferowanych aktualnie przez sieć (sam temat wykorzystania otwartych źródeł do budowy, analizy i weryfikacji sieci powiązań między osobami wymagałby oddzielnej

[63] https://run-log.com/.
[64] http://www.mapmyrun.com.
[65] http://www.endomondo.com.

publikacji o porównywalnej objętości). Nowe aplikacje i serwisy udostępniające nowatorskie funkcje pojawiają się na rynku informatycznym z dużą regularnością, tak więc wymienienie wszystkich aktualnie dostępnych metod i przewidzenie kierunków ich rozwoju nie jest możliwe. Moim zamiarem było jedynie zasygnalizowanie skali zagrożenia i zwrócenie uwagi na konieczność intensyfikacji działań profilaktycznych ukierunkowanych głównie na edukację i zwiększanie świadomości społecznej na temat skali i rodzajów zagrożeń. Warto również zaznaczyć, że te same metody, z których korzystać mogą sprawcy przestępstw, są dostępne dla organów, instytucji i agencji, których zadaniem jest zwalczanie przestępczości i działalność kontrterrorystyczna, a ich funkcjonariusze powinni zdawać sobie sprawę z potencjału, jaki oferują im nowoczesne technologie, i aktywnie z nich korzystać przy wykonywaniu swoich obowiązków służbowych.

Specjaliści z zakresu bezpieczeństwa podkreślają, że bezkrytyczne dzielenie się informacjami prywatnymi w Internecie wystawia użytkowników na ogromne ryzyko. Już w początkowym okresie rozwoju Sieci 2.0 (ery portali społecznościowych) zwracano uwagę, że „użytkownicy publikują wiele danych osobistych na swój temat, w tym informacji w rodzaju tych, które wykorzystywane są przez instytucje finansowe do weryfikacji tożsamości klientów. (…) Wszystkie strony internetowe zawierające dane osobowe powinny znaleźć się w ogniu krytyki; dotyczy to także stron firmowych publikujących szczegóły biograficzne i CV pracowników. Prostym rozwiązaniem jest usunięcie wszystkich danych prywatnych ze wszystkich stron w Internecie, podważa to jednak cel istnienia tych stron: większość użytkowników portali społecznościowych znajduje przyjemność w publikowaniu informacji, w tym tych osobistych”[66]. Mimo upływu lat ostatnie zacytowane zdanie pozostaje boleśnie aktualne. Jak zauważa profesor prawa internetowego z Uniwersytetu Harvarda Jonathan Zittrain: „Gdyby Internet został zaprojektowany wokół koncepcji zapewnienia bezpieczeństwa, nigdy nie osiągnąłby tak wielkiego sukcesu, jakim cieszył się już nawet w 1988 roku. Podstawowym założeniem projektowania i wdrażania protokołu internetowego było po prostu przypuszczenie, że ludzie będą z niego korzystać w sposób rozsądny”[67]. Być może końcowa konstatacja wyda się Czytelnikom nadto brutalna, ale dopóki ludzie nie pozbędą się przywar pychy, nieroztropności i ignorancji, dopóty będą się stawać łatwymi ofiarami przestępstw – w tym przypadku: internetowych. Niestety, jestem w tym zakresie pesymistą.

Streszczenie

Artykuł prezentuje problematykę kryminalistyczną otwartych źródeł informacji (tzw. białego wywiadu) pochodzących z Internetu. Przedstawia możliwości taktycznego i strategicznego wykorzystania tych źródeł przez organa ścigania. Zwraca również uwagę na zagrożenia wynikające z niekontrolowanego dostępu do informacji i perspektyw skorzystania z nich przez sprawców przestępstw i terrorystów.

[66] A. Marshall, P. Stephens, *Identity and identity theft*, w: R. Bryant (red.), *Investigating Digital Crimes*, Wiley, Chichester 2008, s. 188–189.
[67] J. Zittrain, op. cit., s. 60.

Słowa kluczowe: biały wywiad, otwarte źródła informacji, *open source intelligence*, OSInt, Internet, cyberprzestrzeń, cyberprzestępczość, cyberterroryzm, *cyberspace*, *cybercrime*, *cyberterrorism*, sieci społecznościowe, *social networks*, policja, służby specjalne, terroryzm, przestępczość kryminalna, bezpieczeństwo

Summary

The paper presents the forensic aspects of Open Source Intelligence, specifically the Internet-based OSInt. It offers the description of the opportunities for the tactical and strategic use of such sources by the law-enforcement agencies. Additionally, it is focused on the threat assessment of the risks arising from the uncontrolled access to information and its potential illicit use by the criminal offenders and terrorists.

Keywords: open source intelligence, open source information, OSInt, Internet, cyberspace, cybercrime, cyberterrorism, social networks, police, law enforcement agencies, terrorism, crime, security.