ACTA IURIDICA RESOVIENSIA Nr 4(39)/2022
ISSN 2720-0574 DOI: 10.15584/actaires.2022.4.9

Marcin Konieczny

Wyższa Szkoła Policji w Szczytnie
ORCID: 0000-0002-1798-1509

WYKORZYSTANIE TECHNIKI SOCMINT. W ZWALCZANIU CYBERPRZESTĘPCZOŚCI

Wprowadzenie

Według raportu firmy Hootsuite dotyczącego mediów społecznościowych na świecie oraz w poszczególnych krajach z internetu w Polsce korzysta 31,97 mln osób, czyli 84,5% całkowitej populacji (stan na styczeń 2021 r.). Mediów społecznościowych używa 25,9 mln osób, czyli zdecydowana większość populacji naszego kraju (68,5%). Porównując te dane z wynikami 2020 r., liczba użytkowników social media wzrosła aż o 2,5 mln, czyli 11%[1].

Powyższe liczby wskazują na to, że media społecznościowe odgrywają w życiu społeczeństwa ogromną rolę. Stanowią źródło informacji i rozrywki. Są powszechnym kanałem komunikacji, zarówno prywatnej, jak i zawodowej. Należy jednak pamiętać, że poza licznymi pozytywami, jakie niesie ze sobą przestrzeń internetowa i media społecznościowe, na użytkowników czyha również wiele zagrożeń.

Celem niniejszego artykułu jest przedstawienie niebezpiecznych aspektów korzystania z mediów społecznościowych i przestępstw popełnianych w internecie, ze szczególnym naciskiem na wszelkie informacje, jakie użytkownicy publikują w sieci. Zaprezentowane zostaną metody wyszukiwania tych informacji na portalach społecznościowych, a także techniki pomagające zwalczać cyberprzestępczość (SOCMInt.).

Zagrożenia dla użytkowników mediów społecznościowych

Media społecznościowe są aplikacjami sieciowymi, które bazują na ideologicznych i technologicznych podstawach Web 2.0. Charakteryzują się bardzo wysokim stopniem interaktywności użytkowników, a podstawą ich funkcjono-

[1] *Social Media w Polsce 2021 – nowy raport*, https://empemedia.pl/social-media-w-polsce-2021-nowy-raport/ (27.07.2021).

wania jest możliwość tworzenia i wymieniania treści generowanych przez użytkowników. Istotny jest zatem twórczy charakter mediów społecznościowych, dzięki którym człowiek może aktywnie wyrażać swoje poglądy, okazywać emocje i udostępniać je szerokiemu gronu użytkowników[2].

Media społecznościowe są skarbnicą wiedzy na wiele tematów. Można podzielić je na kilka ogólnych grup[3]:

- informacje osobiste o użytkownikach, w tym informacje o sytuacji majątkowej, statusie związku, miejscu zamieszkania, wieku, pracy, orientacji seksualnej, relacji z najbliższym otoczeniem czy poglądach,
- informacje o firmach i organizacjach, np. te publikowane przez obecnych lub byłych pracowników, klientów,
- informacje związane z aktualnymi wydarzeniami w kraju i na świecie,
- informacje na temat różnych zjawisk, zagadnień, które są w obszarze zainteresowania danego użytkownika.

Poprzez udostępniane w mediach społecznościowych informacje (wszelkiego charakteru) użytkownicy czynią niejako sieci społecznościowe dobrym kanałem komunikacji dla przestępców i oszustów. Media społecznościowe zaprojektowane zostały w taki sposób, aby umożliwić użytkownikowi dzielenie się ze światem materiałami powstałymi w sposób swobodny, aby pobudzić ekspresję użytkownika. Ekspresję i swobodę tę widać szczególnie w zakresie informacji udostępnianych przez użytkowników. Są to zazwyczaj pewne poglądy, opinie, zdjęcia, wydarzenia z życia prywatnego. W przypadku wielu użytkowników zauważyć można tzw. *over-sharing*, czyli „naddzielanie się" informacjami prywatnymi. Zjawisko to zwiększa ryzyko stania się ofiarą działań przestępczych[4].

Na użytkowników mediów społecznościowych czyha bardzo wiele zagrożeń, m.in. różnego rodzaju manipulacje, cyberprzemoc, kradzież tożsamości, włamania na prywatne konta i szeroko rozumiane oszustwa internetowe.

„Jedną z technik popełniania przestępstw internetowych jest tzw. kradzież tożsamości, która bezpośrednio łączy się z przetwarzaniem danych osobowych, które to uregulowane jest przepisami ustawy o ochronie danych osobowych. Podstawowym założeniem sprawców posługujących się tą techniką jest bowiem pozyskiwanie jak największej ilości danych osobowych, które następnie wykorzystywane są w celu popełnienia czynów zabronionych. Zgodnie z art. 6 ust. 1 ustawy o ochronie danych osobowych[5] (u.o.d.o.), za dane osobowe uważa się wszelkie informacje

[2] M. Iwanowska, *Zrozumieć media społecznościowe. Perspektywa psychologiczna* [w:] *Media, biznes, kultura. Rzeczywistość medialna. Formy, problemy, aspiracje*, red. M. Łosiewicz, A. Ryłko-Kurpiewska, Gdynia 2016, s. 6.

[3] P. Hrabiec-Hojda, *Techniki wyszukiwania informacji w mediach społecznościowych dla celów białego wywiadu*, „Studia i Analizy" 2019, nr 54, s. 178.

[4] *Vademecum bezpieczeństwa informacyjnego*, red. O. Wasiuta, R. Klepka, Kraków 2019, s. 362–363.

[5] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000).

dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W dalszej części przepisu ustawa precyzuje, iż osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne"[6]. Wiek XXI jest czasem socjotechników, którym w szczególny sposób zależy na kradzieży tożsamości innych osób. Ataki internetowe, których celem jest pozyskanie pożądanych danych, dzielą się na dwie grupy[7]:

1. Pierwsza grupa ataków opiera się na tym, że atakujący postępuje według scenariusza, który traktuje internet i media społecznościowe jako źródło komunikacji. Nie muszą oni posiadać rozbudowanej wiedzy informatycznej, zazwyczaj nie są hakerami.
2. Druga grupa ataków dotyczy głównie socjotechników-hakerów, którzy tworzą złośliwe oprogramowania. Muszą oni posiadać bogatą wiedzę informatyczną ze względu na przebiegłość działania.

T. Trejderowski wyróżnia takie rodzaje złośliwych oprogramowań, którymi posługują się socjotechnicy-hakerzy[8]:

- oprogramowania udostępniane w sieci typu *peer-to-peer*,
- rozszerzenia do popularnych przeglądarek internetowych,
- programy instalujące dodatkowe paski narzędziowe w przeglądarkach WWW,
- fałszywe sterowniki do urządzeń, które są zainstalowane na komputerze,
- programy, które z zasady mają ulepszyć pracę komputera, np. antywirusy,
- załączniki do e-maili, które bazują na emocjach i regułach socjotechnicznych, np. obrazki, wygaszacze ekranu.

Zapewne większość użytkowników spotkała się z wyżej wymienionymi programami. Jest to jeden rodzaj niebezpieczeństw związanych z możliwością kradzieży danych. Drugim są sami użytkownicy internetu, którzy poprzez zamieszczane w sieci informacje mogą sami siebie narażać na różnego rodzaju niebezpieczeństwa. „Laurence Lessing, profesor prawa ze Stanford University twierdzi, że w dzisiejszych czasach wszyscy przypominamy ślimaki, które przemieszczając się pozostawiają za sobą wyraźny ślad. Tym śladem są w naszym przypadku prawie wszystkie wykonywane dziś działania związane z nowoczesnymi urządzeniami"[9].

Bardzo często użytkownicy różnych portali społecznościowych stosują jedno hasło do wszystkich lub większości swoich kont. Może to nieść ze sobą wiele negatywnych konsekwencji. Przede wszystkim osoba, która w jakiś sposób pozyska

[6] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 250–251.

[7] A. Mirski, M. Barcik, M. Gawron, *Kradzież tożsamości w Internecie*, „Człowiek Społeczny w Przestrzeni Internetu" 2015, nr 4, s. 218.

[8] T. Trejderowski, *Kradzież tożsamości*, Warszawa 2013, s. 55.

[9] *Ibidem*, s. 98.

te dane, ma automatycznie dostęp do wszystkich serwisów danego użytkownika. Jedną z form kradzieży danych, o której należy wspomnieć, jest phishing. Polega on na tym, że dany użytkownik internetu może być w pewien sposób „zwabiony" na konkretne strony WWW, które są odpowiednio sfałszowane. Często są to takie strony, które zachęcają użytkownika do pozostawienia swoich danych, w tym haseł. Ciekawy przykład kradzieży haseł dotyczy popularnej gry „World of Warcraft". Gracz logujący się do tej gry mógł stać się ofiarą pozyskania jego danych logowania przez odpowiednio przygotowane złośliwe oprogramowania. Kolejną niebezpieczną techniką kradzieży danych jest stosowanie tzw. keyloggerów. Metoda ta została opracowana na uniwersytecie Georgia Tech. Polega na tym, że oprogramowanie rozpoznaje znaki, które wprowadzane są na konkretnym urządzeniu wyposażonym w akcelerometr. System operacyjny tego urządzenia z reguły nie jest zabezpieczony przed takim atakiem, dlatego funkcje keyloggera może posiadać prawie każda aplikacja zainstalowana na smartfonie[10].

Istnieje wiele aplikacji, które z pozoru mają ułatwić użytkownikom korzystanie z portali społecznościowych, a w rzeczywistości niosą ze sobą wiele zagrożeń. Przykładem może być aplikacja, która po zalogowaniu miała rzekomo pokazać użytkownikowi, kto odwiedzał jego profil – Profile Visitors. W rzeczywistości przestępcy internetowi wysyłają do użytkowników wiadomość z informacją o osobach przeglądających ich profile, ale okazuje się, że lista tych osób będzie dostępna dopiero po zalogowaniu się do serwisu. Po tej czynności użytkownik przekazuje automatycznie dane swojego logowania wraz z listą swoich znajomych. Klikając facebookowe „Lubię to", również można dostarczyć sprytnemu socjotechnikowi wiele danych. Można przekazać mu informacje na temat swoich zainteresowań, preferencji, ludzi, z którymi utrzymuje się relacje. Socjotechnik, udając, że ma takie same zainteresowania, może próbować nawiązać kontakt ze swoją „ofiarą" i pozyskać przez to jeszcze więcej interesujących go danych[11].

Dużym zagrożeniem czyhającym na użytkowników internetu, a w szczególności mediów społecznościowych, jest cyberprzemoc. Jest to stosowana za pomocą sieci internetowych i technologii elektronicznych przemoc względem innych osób. Osoba, która dopuszcza się takich czynów, to stalker, a osoba atakowana to ofiara. Cyberprzemoc może prowadzić do bardzo poważnych skutków, m.in. samobójstwa osób poniżanych lub zastraszanych w sieci. Cyberprzemocą jest[12]:

- *flaming,* czyli agresywna wymiana zdań na czacie lub w grupach dyskusyjnych,
- prześladowanie, czyli regularne przesyłanie użytkownikowi (ofierze) treści obraźliwych, najczęściej za pomocą komunikatorów internetowych,
- maskarada, czyli tworzenie fałszywych profili danej osoby np. na portalach społecznościowych, aby jej zaszkodzić,

[10] A. Mirski, M. Barcik, M. Gawron, *Kradzież tożsamości*…, s. 220.

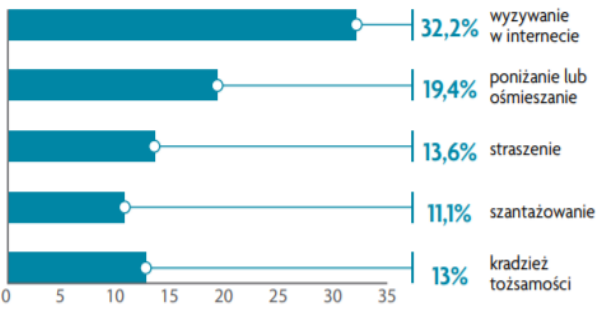
[11] *Ibidem,* s. 222.

[12] D. Siemieniecka, M. Skibińska, K. Majewska, *Cyberagresja – zjawisko, skutki, zapobieganie*, Toruń 2020, s. 20–21.

– *trolling*, czyli umieszczanie dużej ilości złośliwych, obraźliwych, poniżających treści przez sprawcę-trolla na temat swojej ofiary,
– *flood*, czyli zapychanie skrzynki ofiary przez trolla niechcianymi wiadomościami,
– *sexting*, czyli rozsyłanie zdjęć, filmów o kontekście erotycznym, seksualnym bez wiedzy i zgody ofiary,
– włamania do miejsca w internecie zabezpieczonego przez użytkownika hasłem w celu uzyskania konkretnych informacji,
– kradzież tożsamości, czyli podszywanie się, podawanie się za pokrzywdzonego po uprzednim włamaniu się np. na konto w portalu społecznościowym i uzyskaniu dostępu do niego – wysyłanie w jego imieniu wiadomości, publikowanie nieprawdziwych treści.

Raport *Cyberprzemoc. Włącz blokadę na nękanie* opracowany przez Państwowy Instytut Badawczy NASK w 2019 r. wskazuje na najczęstsze powody cyberprzemocy. Są to[13]:
– poglądy,
– wygląd,
– upodobania,
– narodowość,
– orientacja seksualna,
– religia,
– kolor skóry,
– płeć,
– zła sytuacja materialna.

Agresja w sieci jest zjawiskiem niemal powszechnym. Ponad połowa młodych użytkowników internetu przyznaje, że pośrednio lub bezpośrednio spotkała się z różnymi formami internetowej przemocy[14].



Wykres 1. Doświadczanie różnych form cyberprzemocy przez nastolatki (13–17 lat)

Źródło: A. Borkowska, *Cyberprzemoc. Włącz blokadę na nękanie*, https://akademia.nask.pl/publikacje/Poradnik_cyberprzemoc_www.pdf (28.07.2021).

[13] A. Borkowska, *Cyberprzemoc. Włącz blokadę na nękanie*, https://akademia.nask.pl/publikacje/Poradnik_cyberprzemoc_www.pdf (28.07.2021).

[14] *Ibidem*.

Na wykresie 1 zaprezentowano dane na temat różnych form cyberprzemocy, której mogli doświadczyć nastolatkowie. Co trzecia młoda osoba (32,2%) przyznaje, że była wyzywana w internecie. 19,4% uczniów twierdzi, że byli poniżani lub ośmieszani. Ponadto 13,6% młodych osób mówi o tym, że byli straszeni w internecie, 11,1% – szantażowani, a 13% młodzieży skradziono tożsamość w sieci.

Cyberprzemoc jest zachowaniem, które może wypełniać znamiona różnych przestępstw zawartych w wielu przepisach k.k., np. zniesławienia (art. 212 § 1 i 2 k.k.), zniewagi (art. 216 § 1 i 2 k.k.), kradzieży tożsamości (art. 268 § 1 k.k.), groźby karalnej (art. 190 § 1 k.k.), uporczywego nękania oraz podszywania się pod inna osobę lub wykorzystywania jej wizerunku (art. 190a § 1 i 2 k.k.)[15]. Często użytkownicy internetu – zwłaszcza ci młodsi – nie zdają sobie sprawy z powagi sytuacji, jaką jest prześladowanie w sieci. Wiele czynności traktują jako zabawę, wygłup, nie zwracając uwagi na negatywne konsekwencje, jakie może to ze sobą nieść. Internet jest miejscem popełniania wielu przestępstw i wszystkie akty cyberprzemocy podlegają odpowiedzialności prawnej.

Poza wszelkimi formami cyberprzemocy użytkownicy mogą również być narażeni na różnego rodzaju oszustwa internetowe. Są to czyny, które łączą w sobie elementy nieuprawnionych działań o charakterze technicznym z wyraźnymi elementami socjotechniki i inżynierii społecznej. Istotą oszustwa internetowego jest takie zastosowanie technik informatycznych, aby wprowadzić użytkownika w błąd dla osiągnięcia konkretnego celu. Oszustwami internetowymi są[16]:

- wyłudzanie danych,
- podsłuchiwanie transmisji danych,
- spowodowanie wykonania przez użytkownika sieci konkretnej czynności, np. dokonanie przelewu bankowego na nieprawdziwy numer konta dostępny na sfałszowanej stronie internetowej,
- wprowadzenie do systemu ofiary szkodliwego oprogramowania,
- włączenie urządzenia ofiary do sieci komputerów zombie, czyli tzw. botnetu, który następnie wykorzystywany jest przez zorganizowane grupy przestępcze do popełniania cyberataków.

Powyższy katalog oszustw internetowych nie jest oczywiście zamknięty. Wraz z rozwojem nowych technologii jego zakres ciągle poszerza się o nowe formy przestępstw. Jedną z głównych metod stosowanych do przeprowadzania wszelkiego rodzaju oszustw internetowych jest stosowanie tzw. inżynierii społecznej. Metoda ta opiera się na założeniu, że często łatwiej jest wykorzystać ludzką naiwność lub niewiedzę, nić łamać nowoczesne zabezpieczenia informatyczne. „Jeden z największych oszustów komputerowych wszechczasów, aktual-

[15] *Cyberprzemoc*, file:///C:/Users/Admin/Downloads/Cyberprzemoc.pdf (28.07.2021).

[16] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Białystok 2017, s. 288.

nie uznany konsultant bezpieczeństwa systemów teleinformatycznych, przyznaje, że nie ma sensu łamać haseł do komputerów, skoro można poprosić o nie ich użytkowników”[17]. Istotą komputerowej inżynierii społecznej jest dokonanie manipulacji na ludziach, tzn. podszycie się pod inną osobę, wprowadzenie użytkownika w błąd i ostatecznie nakłonienie go do dobrowolnego poddania się konkretnemu oszustwu, praktycznie bez jego wiedzy. Z technicznego punktu widzenia najbardziej popularnymi sposobami działania cyberprzestępców jest przygotowanie odpowiedniej wiadomości, strony internetowej, która swoim wyglądem przypominała będzie realną, rzeczywistą stronę, np. banku. Skopiowanie szaty graficznej strony internetowej jest w zasadzie dosyć prostym zabiegiem. Jeśli więc użytkownik nie zorientuje się, że adres internetowy konkretnej strony uległ choćby drobnej zmianie, jest w stanie wpisać swoje poufne dane i tym sposobem przekazać je oszustowi. Przygotowanie takiego nielegalnego zabiegu wymaga często pozyskania określonej wiedzy na temat użytkownika (ofiary) przez oszusta. Co ciekawe, źródłem takich informacji lub dużą pomocą mogą być treści publikowane przez potencjalne ofiary w portalach społecznościowych[18].

Metody wyszukiwania informacji w mediach społecznościowych

W celu pozyskania informacji z mediów społecznościowych dotyczących konkretnej osoby można użyć takich metod, jak[19]:

- bezpośrednie wyszukiwanie konkretnych informacji udostępnionych publicznie w mediach społecznościowych za pomocą wewnętrznej wyszukiwarki lub wyszukiwania zaawansowanego,
- wyszukiwanie za pomocą zewnętrznych narzędzi, które poprzez wpięcie API do mediów społecznościowych pozwalają pobierać i strukturyzować dane lub za pomocą zewnętrznych narzędzi, które tworzą zaawansowane kwerendy wyszukiwawcze w Google,
- wyszukiwanie danych w wyszukiwarce z wykorzystaniem zaawansowanych operatorów i technik.

Bezpośrednie wyszukiwanie informacji publicznych na Facebooku, Twitterze czy Instagramie jest dosyć prostym zabiegiem. Social media generują jednak tak ogromne ilości danych, że pozwalają one na powstawanie specjalistycznych aplikacji i programów komputerowych, których zadaniem jest monitorowanie konkretnych informacji. „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 społeczno-

[17] *Ibidem*, s. 289.
[18] *Ibidem*.
[19] P. Hrabiec-Hojda, *Techniki wyszukiwania*…, s. 180.

ściowym”[20]. W związku z tym warto zaprezentować kilka wybranych narzędzi ułatwiających pozyskanie informacji dostępnych w mediach społecznościowych[21]:

1. Stalkscan, czyli aplikacja, której zadaniem jest ukazanie facebookowego profilu użytkownika „w kawałkach”. Jest ona szczególnie pomocna w przypadku użytkowników, którzy wykazują się dużą aktywnością w social mediach.
2. Search is back, podobnie jak Stalkscan, jest aplikacją pomagającą wyszukać konkretne informacje na temat użytkownika – dane osobowe, zdjęcia, wydarzenia, posty z zastosowaniem poszczególnych filtrów dla uzyskania jak najbardziej precyzyjnych informacji (miejsca zamieszkania, pracy itp.). Dodatkowym wymiarem jest określenie przestrzeni czasowej, tzn. czy przedmiotem zainteresowania są wydarzenia obecne, czy może te z przeszłości.
3. Recruitin.net, czyli narzędzie, które stanowi pewnego rodzaju nakładkę na Google ułatwiającą wpisywanie zaawansowanych kwerend w wyszukiwarce, koncentrując się głównie na portalach LinkedIn czy Twitter.
4. Onemilliontweetmap.com, czyli aplikacja, która łączy w sobie dwa trendy w podejściu do pozyskiwania informacji: nieustanny monitoring i wizualizację. Na interaktywnej mapie osoba poszukująca informacji otrzymuje wizualizację intensywności życia użytkownika na Twitterze w czasie rzeczywistym.
5. Twitonomy to aplikacja, która pozwala na monitorowanie wybranych kont na Twitterze w czasie rzeczywistym.

Przedstawione powyżej narzędzia pozwalają przeszukać i zdobyć informacje zamieszczone na portalach społecznościowych. Jest to jednak niewielka część wszystkich narzędzi służących temu celu, które bardzo często są zmieniane i udoskonalane[22].

Techniki SOCMInt. w walce z cyberprzestępczością

SOCMInt., czyli inteligencja mediów społecznościowych (*social media intelligence*), to wykorzystywanie różnych technik w celu pozyskania pożądanych informacji z mediów społecznościowych. Odnosi się w szczególności do narzędzi, które mają pomóc konkretnym instytucjom monitorować kanały społecznościowe. Istotą działania SOCMInt. jest „zaplanowane i zorganizowane pozyskanie, przetworzenie oraz dystrybucja zgromadzonych wiadomości dla określonej grupy odbiorczej, która wcześniej sprecyzowała zainteresowanie danym zakresem informacji (zwykle na potrzeby podjęcia decyzji lub rozwiązania problemu)”[23].

[20] P. Karasek, *Analiza informacji z mediów społecznościowych jako narzędzie wspierające kontrolę bezpieczeństwa w procedurach migracyjnych*, „Przegląd Bezpieczeństwa Wewnętrznego” 2018, nr 19, s. 201.

[21] P. Hrabiec-Hojda, *Techniki wyszukiwania*…, s. 182–188.

[22] *Ibidem*, s. 188.

[23] *Vademecum bezpieczeństwa informacyjnego*, red. O. Wasiuta, R. Klepka, Kraków 2019, s. 362–363.

Media społecznościowe umożliwiają gromadzenie danych wywiadowczych i śledczych. Ten typ gromadzenia tych danych jest jednym z elementów OSInt. (*open source intelligence*), czyli otwartego oprogramowania wywiadowczego, który polega na pozyskiwaniu i gromadzeniu informacji z otwartych źródeł[24]. SOCMInt. obejmuje działania z zakresu zarówno białego, jak i czarnego wywiadu. Jeśli chodzi o ten pierwszy, odnosi się on do korzystania z różnego typu materiałów i informacji publikowanych w mediach społecznościowych przez konkretnych użytkowników. Drugi natomiast dotyczy administratorów poszczególnych serwisów społecznościowych, konkretnych urządzeń i kont użytkowników. Pozyskiwanie informacji z tych źródeł może się odbywać na podstawie konkretnych regulacji prawnych, które mają umożliwić organom ścigania takie działania wyłącznie na potrzeby prowadzonego śledztwa, dochodzenia[25].

Służby wywiadowcze wykorzystują SOCMInt. m.in. do[26]:

- analizowania i monitorowania zagrożeń szczególnie istotnych, np. terroryzmu,
- gromadzenia informacji o osobach prywatnych i firmach na poziomie lokalnym,
- analizowania informacji na temat konkretnych wydarzeń,
- monitorowania społeczeństwa.

W obszarze zainteresowania SOCMInt. pozostają[27]:

1. *Social mobile*, czyli dostęp do informacji zawartych w mediach społecznościowych poprzez smartfon. Jest to pewnego rodzaju rewolucja internetowa. Łącza bezprzewodowe pozwalają na obecność w sieci w zasadzie bez żadnych ograniczeń czasowych i miejscowych. Wymiana informacji za pomocą mediów społecznościowych również może odbywać się bez żadnych ograniczeń, np. na terenie państw członkowskich Unii Europejskiej każdy ma wolny, w zasadzie nieograniczony dostęp do sieci internetowych. Użytkownicy udostępniają w ten sposób ważne informacje na temat miejsca pobytu, nastroju itp.
2. Wyszukiwarki społecznościowe, a w szczególności największa z nich, czyli Google. Zastosowanie konkretnego algorytmu pozwala doskonale pozycjonować strony internetowe i tym samym pozyskiwać najbardziej pożądane informacje.
3. Geotargetowanie, czyli pozostawianie w sieci śladów aktywności, a przede wszystkim informacji o tym, w jakim miejscu konkretna osoba aktualnie się znajduje. W ostatnich latach zaobserwować można wyraźny wzrost zainteresowaniem kwestiami związanymi z geotargetowaniem. Ma to niewątpliwie związek z rozwojem internetu mobilnego i smartfonów.
4. *E-commerce* w social mediach. Bardzo dużo znanych marek, a także mniejszych lub nawet początkujących firm sprzedaje swoje produkty w social mediach. Przykładowo Facebook umożliwia użytkownikom zakup wszelkiego

[24] *Ibidem*.
[25] P. Waszkiewicz, *Media społecznościowe w pracy organów ścigania*, Warszawa 2021, s. 10.
[26] *Vademecum bezpieczeństwa informacyjnego*, red. O. Wasiuta, R. Klepka, Kraków 2019, s. 364.
[27] *Ibidem*, s. 366.

rodzaju produktów. Co więcej, odpowiednie algorytmy, śledząc użytkowników, przedstawiają im odpowiednie rekomendacje produktowe w różnych miejscach w internecie. Na przykład użytkownik przegląda konkretne oferty danego sklepu, a produkty, którymi był zainteresowany, pojawiają się w formie przypomnienia jako reklama dynamiczna na Facebooku, Messengerze lub Instagramie.

5. *Social gaming*, czyli możliwość grania w sieci ze znajomymi.

Należy pamiętać o tym, że logując się w różnych serwisach i aplikacjach internetowych, użytkownicy zostawiają po sobie „ślad", który następnie jest wykorzystywany w celu identyfikacji, rozpoznania preferencji, pozyskania informacji czy nawiązania potencjalnego kontaktu. Istnieją narzędzia w social media, które dzięki sztucznej inteligencji pozwalają rozpoznać i dopasować odpowiednie treści do konkretnego użytkownika zgodnie z jego preferencjami poprzez[28]:

1. Rozpoznanie głosu – przykładem może być Siri w urządzeniach posiadających oprogramowanie iOS, która pełni funkcje osobistego asystenta. Wykonuje różne zadania i odpowiada na wszelkie zapytania właściciela smartfonu.
2. Rozpoznanie tekstu poprzez analizę danych możliwe jest rozpoznanie aktualnych trendów i pozycjonowanie ich.
3. Rozpoznawanie obrazu.

SOCMInt. skupia się wokół informacji prywatnych najczęściej udostępnionych dobrowolnie przez samego użytkownika w mediach społecznościowych (Facebook, Instagram, Twitter). „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"[29].

Pojęcie SOCMInt. po raz pierwszy zostało zaproponowane w 2012 r. przez D. Omanda, S. Barletta i C. Millera w cyklu artykułów stworzonych dla londyńskiej organizacji non profit Demos. Autorzy zgodnie twierdzili, że media społecznościowe są aktualnie bardzo ważnym elementem w pracy wywiadowczej, ale zanim będzie można uznawać je za nową formę inteligencji, należy dopracować brytyjską ustawę z 2000 r. o uprawnieniach dochodzeniowo-śledczych. W dokumencie tym określono uprawnienia organów publicznych do nadzorowania, prowadzenia dochodzeń i dostępu do wszelkiej komunikacji elektronicznej, a także przechwytywania danych dotyczących konkretnej osoby[30].

SOCMInt. stanowi część cyfrowej inteligencji, która z kolei jest bardzo ważnym źródłem informacji dla policji i struktur bezpieczeństwa wielu krajów na temat tożsamości czy lokalizacji osób podejrzanych o popełnienie danego przestępstwa. Wykorzystanie mediów społecznościowych do celów taktycznych

[28] *Ibidem.*

[29] P. Karasek, *Analiza informacji…*, s. 200.

[30] *Vademecum bezpieczeństwa informacyjnego*, red. O. Wasiuta, R. Klepka, Kraków 2019, s. 364.

i wywiadowczych, a także pojawianie się coraz to nowszych techniki pozwala na zwalczanie cyberprzestępczości[31].

Monitoring mediów społecznościowych musi się opierać na odpowiednich podstawach prawnych. Należy pamiętać jednak, że bez tego monitoringu i przechowywania danych o użytkownikach i ich aktywnościach w social mediach (czyli bez stosowania technik SOCMInt.) internet mógłby stać się miejscem pełnym jeszcze większej ilości niebezpieczeństw i przestępstw. Media społecznościowe są zatem monitorowane przez policję i służby bezpieczeństwa, ponieważ są nową przestrzenią publiczną, w której większość społeczeństwa spędza wiele czasu. Wiąże się to z tym, że media społecznościowe stały się miejscem popełniania przestępstw, np. pedofilii lub aktów terrorystycznych. Wykorzystywanie technik SOCMInt. w przestrzeni internetowej ma zatem decydujący wpływ na całokształt bezpieczeństwa narodowego[32]:

- wspiera zwalczanie działalności przestępczej,
- pomaga we wczesnym ostrzeganiu społeczeństwa przed konkretnymi zagrożeniami,
- buduje świadomość sytuacyjną w dynamicznie zmieniających się okolicznościach.

Podsumowanie

Przedstawione w niniejszym artykule metody popełniania przestępstw w internecie, a także ich skala wskazują wprost na powszechność zjawiska cyberprzestępczości. Załączone dane statystyczne dotyczące korzystania z internetu (a przede wszystkim z mediów społecznościowych) dają podstawę ku temu, by twierdzić, że social media są pewną nowoczesną, obszerną przestrzenią publiczną. Poza wieloma pozytywnymi aspektami, jakie wynikają z korzystania z mediów społecznościowych, należy również pamiętać, że poprzez swoją powszechność są one miejscem popełniania wielu przestępstw. Użytkownicy często publikują w sieci prywatne informacje, których nie ujawniliby tak łatwo nieznanym osobom w świecie rzeczywistym. Częsty brak rozwagi w publikowanych treściach może nieść ze sobą wiele negatywnych konsekwencji dla samego autora publikowanych treści, takich jak cyberprzemoc, kradzież tożsamości, kradzież danych i szeroko rozumiana manipulacja i oszustwa internetowe.

SOCMInt., czyli inteligencja mediów społecznościowych, to wykorzystywanie różnych technik w celu pozyskania pożądanych informacji z mediów społecznościowych. Odnosi się w szczególności do narzędzi, które mają pomóc konkretnym instytucjom monitorować kanały społecznościowe. Wykorzystanie technik SOCMInt. przez policję i inne organy bezpieczeństwa pomaga zwalczać i zapobiegać przestępstwom internetowym.

[31] *Ibidem.*

[32] D. Siemieniecka, M. Skibińska, K. Majewska, *Cyberagresja – zjawisko*…, s. 23.

Techniki SOCMInt. mają zarówno wielu sprzymierzeńców, jak i przeciwników. Ci drudzy uważają, że zastosowane technologie w ramach działania SOCMInt. wykraczają poza ramy działalności OSInt., czyli zbierania wszelkich danych z publicznych źródeł, które dostępne mają być docelowo dla wszystkich. Użytkownicy mediów społecznościowych bardzo często udostępniają dane tylko zaakceptowanym przez siebie użytkownikom (dodanym do znajomych). Organy ścigania bardzo często pozyskują takie informacje z kont fikcyjnych, do których założenia użytkownik wykorzystuje nieprawdziwe dane. Przeciwnicy SOCMInt. uważają, że jest to nadużycie i nieuprawnione wnikanie w prywatność użytkowników social media, a także daleko idąca inwigilacja. Służby stosujące techniki SOCMInt. odpierają jednak te zarzuty, wskazując na to, że ich działania polegają przede wszystkim na analizie treści udostępnionych publicznie.

Można rozważać pozytywne i negatywne aspekty zastosowania techniki SOCMInt. przez organy ścigania. Być może dla wielu użytkowników internetu jest to nadmierna inwigilacja. Z drugiej strony jednak bez odpowiedniego monitorowania i analizowania treści zamieszczonych w internecie stałby się on miejscem popełniania jeszcze większej ilości przestępstw. Techniki SOCMInt. zdecydowanie pomagają organom ścigania w zwalczaniu cyberprzestępczości.

Analiza zagadnień związanych z korzystaniem z mediów społecznościowych i towarzyszących temu możliwości stania się ofiarą przestępstwa pozwoliła ustalić, że występuje luka w przepisach prawa, które nie uwzględniają w obecnym kształcie pojęcia cyberprzemocy jako przestępstwa, a jedynie wskazują, iż za przestępstwo można uznać pewne zachowania mieszczące się w ramach tego zjawiska. Podobnie aktualny stan prawny nie uwzględnia zjawiska przestępstwa internetowego, pomimo iż z takim służby spotykają się coraz częściej. Rozwój technologii i związanych z tym możliwości popełniania przestępstw wymaga zatem wprowadzenia nowych pojęć do k.k. i dokładnego ich zdefiniowania.

Bibliografia

Hrabiec-Hojda P., *Techniki wyszukiwania informacji w mediach społecznościowych dla celów białego wywiadu*, „Studia i Analizy" 2019, nr 54.

Iwanowska M., *Zrozumieć media społecznościowe. Perspektywa psychologiczna* [w:] *Media, biznes, kultura. Rzeczywistość medialna. Formy, problemy, aspiracje*, red. M. Łosiewicz, A. Ryłko-Kurpiewska, Gdynia 2016.

Karasek P., *Analiza informacji z mediów społecznościowych jako narzędzie wspierające kontrolę bezpieczeństwa w procedurach migracyjnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19.

Mirski A., Barcik M., Gawron M., *Kradzież tożsamości w Internecie*, „Człowiek Społeczny w Przestrzeni Internetu" 2015, nr 4.

Siemieniecka D., Skibińska M., Majewska K., *Cyberagresja – zjawisko, skutki, zapobieganie*, Toruń 2020.

Social Media w Polsce 2021 – nowy raport, https://empemedia.pl/social-media-w-polsce-2021--nowy-raport/ (27.07.2021).
Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.
Trejderowski T., *Kradzież tożsamości*, Warszawa 2013.

Streszczenie

Media społecznościowe odgrywają ważną rolę w życiu niemal każdego człowieka. Użytkownicy, publikując konkretne materiały ze swojego życia prywatnego, dostarczają cennej wiedzy internetowym przestępcom. Są przez to narażeni na różne formy cyberprzestępstw, m.in. kradzież tożsamości, cyberprzemoc, oszustwa internetowe. Media społecznościowe muszą być zatem monitorowane przez policję i służby bezpieczeństwa. Wykorzystywanie technik SOCMInt. w przestrzeni internetowej ma decydujący wpływ na całokształt bezpieczeństwa narodowego. W niniejszym artykule przedstawiono niebezpieczeństwa czekające na użytkowników mediów społecznościowych i nowoczesne metody pozyskiwania informacji. Omówiono także najważniejsze kwestie związane z technikami SOCMInt.

Słowa kluczowe: media społecznościowe, cyberprzestępstwa, SOCMInt.

THE USE OF SOCMINT. IN FIGHTING CYBER CRIME

Summary

Social media plays an important role in almost everyone's life. Users by publishing specific materials from their private lives provide valuable knowledge to online criminals. As a result, they are exposed to various forms of cybercrime, including identity theft, cyberbullying, and internet fraud. Therefore, social media must be monitored by the police and security services. Using SOCMInt. techniques. in the Internet space, it has a decisive influence on the overall national security. This article presents the dangers waiting for social media users and modern methods of obtaining information. The most important issues related to SOCMInt. techniques were also discussed.

Keywords: social media, cybercrime, SOCMInt.