Jerzy Surma

Znaczenie analiz sieci społecznych online dla bezpieczeństwa narodowego

Rozwój technologii informatycznych, w tym szczególnie Web 2.0[1], zaowocował powstaniem sieci społecznych online (ang. *social network sites*)[2] w ramach szerszego zjawiska technologiczno-społecznego nazywanego potocznie mediami społecznościowymi (ang. *social media*). Tego typu media umożliwiają użytkownikom tworzenie, współdzielenie i wymienianie wiadomości, opinii, zdjęć, linków itp. w społecznościach wirtualnych[3]. Pod pojęciem mediów społecznościowych należy rozumieć m.in.: blogi, fora internetowe, sieci społeczne online, serwisy współdzielenia zdjęć, serwisy współdzielenia filmów wideo, portale oceny produktów, sklepy online z rekomendacjami i ocenami klientów, serwisy informacyjne z komentarzami, gry online oraz światy wirtualne.

Możliwość łatwego i taniego publikowania oraz wymiany informacji pomiędzy ludźmi pociąga za sobą wiele skutków, z których dwa mają szczególne znaczenie w kontekście bezpieczeństwa narodowego. Pierwszym jest coraz większy wpływ mediów społecznościowych, wypierających klasyczne media (TV, radio, prasę)[4] na rozpowszechnianie informacji oraz zachowania społeczne. Jedne z najbardziej spektakularnych przykładów tego typu wpływu to: wykorzystywanie Twittera w kampanii prezydenckiej w Stanach Zjednoczonych w 2008 r.[5], Facebooka w czasie „arabskiej wiosny" w 2010 r.[6] oraz YouTube'a przez islamistyczne ugrupowanie terrorystyczne ISIS w 2015 r.[7] Drugim skutkiem jest pozostawianie przez użytkowników Internetu tzw. śladów elektronicznych (ang. *digital footprints*), które można przechowywać i analizować[8]. Te dwa rezultaty wymiany informacji mają fundamentalny wpływ na bezpieczeństwo narodowe w zakresie **identyfikacji wojny informacyjnej**[9] prowadzonej z wykorzystaniem mediów społecznościowych. Taka identyfikacja jest możliwa dzięki

[1] Narzędzia Web 2.0 pozwalają na aktywne korzystanie z Internetu przez udostępnianie narzędzi do tworzenia i wymiany treści generowanych samodzielnie przez użytkowników.

[2] Sieć społeczna online jest serwisem internetowym, dzięki któremu użytkownicy mogą: tworzyć publiczne i ukryte profile użytkownika, tworzyć listy innych użytkowników (znajomych), z którymi pragnie się utrzymywać kontakt, przeglądać listy znajomych, za: D.M. Boyd, N.B. Ellison, *Social network sites: Definition, history, and scholarship*, „Journal of Computer-Mediated Communication" 2007, nr 13, s. 210–230.

[3] A.M. Kaplan, M. Haenlein, *Users of the world, unite! The challenges and opportunities of social media* „Business Horizons" 2010, nr 53, s. 59–68.

[4] Według badania YouGov wykonanego w 2013 r. w Stanach Zjednoczonych 29%. badanych w przedziale wiekowym 18–24 nie czytała w danym roku ani razu wydrukowanej gazety. Jednocześnie 55% badanych w tej samej grupie wiekowej deklarowało czytanie wiadomości z serwisów internetowych co najmniej raz w tygodniu.

[5] A. Hughes, L. Palen, *Twitter adoption and use in mass convergence and emergency events*, „International Journal of Emergency Management" 2009, nr 6, s. 248–260.

[6] W. Ghonim, *Revolution 2.0: The Power of the People Is Greater Than the People in Power: A Memoir*, Boston–New York 2013.

[7] Przykładowe nagranie: https://www.youtube.com/watch?v=eX172j6U_KI. [dostęp: 31 XII 2015].

[8] J. Surma, *The Role of Individual Behavior and Social Influence in Customer Relation Management*, w: *Handbook of Research on Managing and Influencing Consumer Behavior*, New York 2015, s. 385–396

[9] Wszystkie wyróżnienia w artykule pochodzą od autora – przyp. red.

analizie jakościowej publikowanych treści oraz wykorzystaniu metod eksploracji danych (ang. *data mining*), w tym szczególnie metod ilościowych analizy sieci społecznych (ang. *social networks analysis*)[10]. Należy podkreślić, że pojęcie sieć społeczna jest znacznie szersze od pojęcia sieć społeczna online. Metody ilościowe opracowywane dla sieci społecznych są również możliwe do stosowania dla sieci online, tym bardziej że w tym przypadku sama struktura sieci, dynamika jej zmian oraz wymieniane informacje są automatycznie rejestrowane w systemach informatycznych, co daje olbrzymi potencjał analityczny.

Wykorzystywanie metod ilościowych w analizie sieci społecznych ma jeszcze drugi obszar zastosowania w zakresie bezpieczeństwa narodowego, a mianowicie **rozpoznanie przestępczości zorganizowanej**, np. działalności terrorystycznej. W niniejszym artykule omówiono wspomniane dwa obszary analiz mediów społecznościowych.

Rola mediów społecznościowych w prowadzeniu wojny informacyjnej

Wojna informacyjna ma na celu wpływanie na zachowania społeczeństwa zgodnie z wolą agresora zewnętrznego przez zarządzanie informacją. W ramach metod stosowanych w tego typu wojnach w sposób zorganizowany wykorzystuje się m.in.: manipulowanie informacją, dezinformację i fabrykowanie informacji. Problematyka wojny informacyjnej i metody jej prowadzenia zostały całościowo omówione w monografii R. Brzeskiego[11]. Niezwykle czytelnym przykładem systemowego prowadzenia wojny informacyjnej są działania Federacji Rosyjskiej w ramach tzw. wojny hybrydowej[12] (m.in. podczas operacji krymskiej[13]) oraz różne akcje dezinformacyjne przeprowadzane na terenie Europy[14].

Wykorzystywanie sieci Internet do prowadzenia wojny informacyjnej jest obecnie jedną z najnowszych metod wpływania na decyzje polityczne, ośmieszania postaw patriotycznych, eskalacji napięć społecznych, osłabiania woli walki czy destabilizacji sytuacji gospodarczej. W tym kontekście szczególnie ważne staje się wykorzystanie niezwykle popularnych mediów społecznościowych, które umożliwiają przeprowadzanie celowych kampanii informacyjnych na forach internetowych i w sieciach społecznych online[15] (ang. *trolling*). Te działania obejmują również prowadzenie agentów wpływu oraz inspirowanie tzw. pożytecznych idiotów. Zorganizowane działania w mediach społecznościowych, będące elementem wojny informacyjnej, służą zwykle:

- kompromitowaniu wybranych osób (organizacji) w państwie – ośmieszanie, obrażanie, niszczenie reputacji czy podważanie autorytetu,

[10] S. Wasserman, K. Faust, *Social Network Analysis. Methods and Applications*, Cambridge 1994.

[11] R. Brzeski, *Wojna informacyjna – wojna nowej generacji*, Komorów 2014.

[12] U. Franke, *War by non-military means. Understanding Russian information warfare*, Stockholm 2015 (Report No FOI-R–4065–SE).

[13] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, seria: Punkt Widzenia – Ośrodek Studiów Wschodnich, Warszawa 2014.

[14] S. Samadashvili, *Muzzling the bear: Strategic Defense for Russia's Undeclared Information War on Europe*, Brussels 2015.

[15] Przykłady wykorzystania mediów społecznościowych w wojnie informacyjnej [dostęp: 31 XII 2015]:

- https://gigaom.com/2012/11/19/how-social-media-is-rewriting-the-rules-of-modern-warfare/,
- http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks,
- http://techcrunch.com/2014/10/15/isis-tactics-illustrate-social-medias-new-place-in-modern-war/,
- http://www.dailymail.co.uk/news/article-2749247/ISIS-declares-war-Twitter-Terror-group-warns-employees-assassinated-closing-Islamist-propaganda-accounts.html,
- http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html.

- dezintegrowaniu społeczeństwa[16] – kreowanie kontrowersyjnych i niejednokrotnie fałszywych treści mających dzielić, prowokować konflikty, wywoływać spory itp.,
- generowaniu zgiełku informacyjnego[17] (ang. *deluge of information*) – stwarzanie wrażenia braku możliwości określenia prawdy obiektywnej przez masowe propagowanie sprzecznych wersji wydarzeń, teorii spiskowych, półprawd itp.,
- infiltracji mediów społecznościowych[18] – przejmowanie kontroli nad istniejącymi forami lub budowanie forów internetowych „pod przykryciem" w celu infiltracji określonych grup społecznych, wpływanie na ich działalność, m.in. przez kreowanie wrażenia masowego poparcia lub odrzucenia wybranych idei.

Tego typu zamierzone działania informacyjne w sieciach wywołują intrygujący efekt uboczny nazywany „mgłą wojny informacyjnej"[19] (ang. *fog of information war*), polegający na tym, że informacja raz umieszczona w sieci zaczyna żyć własnym życiem, najczęściej w sposób zupełnie spontaniczny. Pierwotnie opublikowana informacja może ponadto podlegać różnym transformacjom, m.in. modyfikacji, zniekształceniu, wyjęciu z kontekstu lub innym tego typu działaniom.

Przegląd badań naukowych

Media społecznościowe, głównie ze względu na ich niezwykłą popularność, cieszą się ponadprzeciętnym zainteresowaniem środowiska naukowego. W identyfikowaniu wojny informacyjnej mogą być przydatne co najmniej dwa obszary badawcze:

1. Analiza dyfuzji informacji (ang. *information diffusion*).
2. Analiza społeczności (ang. *community analysis*).

Dyfuzja informacji, czyli proces rozprzestrzeniania się informacji w sieci, jest jednym z najważniejszych obszarów badań sieci społecznych online. Reprezentatywny poziom badań w tym zakresie został zaprezentowany w artykule E. Bakshy'ego[20], artykuł A. Guille'a[21] zaś zawiera dobrze przygotowane podsumowanie stanu badań dotyczące dyfuzji informacji w sieciach społecznych online. Szczególnie istotne są badania nad tzw. wpływem otoczenia społecznego[22] (ang. *social influence*) na zachowania ludzi. Wyniki zaawansowanych badań w tym zakresie implikują wiele zastosowań praktycznych, m.in. w biznesie[23]. Na przykład wykorzystywanie systemów rekomendacyjnych[24] oraz identyfikacja liderów opinii jest obecnie jednym ze standardowych zastosowań w marketingu internetowym[25].

---

[16] https://kazwoy.wordpress.com/2015/07/22/internet-i-wojna-informacyjna-prezydenta-putina-raport-akademii-krzyzowa/ [dostęp: 31 XII 2015].

[17] http: //www.politico.com/magazine/story/2015/01/putin-russia-tv-113960 [dostęp: 31 XII 2015].

[18] P.M. Duggan, *Strategic Development of Special Warfare in Cyberspace*, „Joint Force Quarterly" 2015, nr 4, s. 46–53.

[19] M. Jaitner, P.A. Mattsson, *Russian Information Warfare of 2014*, 7th International Conference on Cyber Conflict, NATO CCD COE Publications 2015, s. 29–52.

[20] E. Baksy i in., *The role of social networks in information diffusion*, Proceedings of the 21 International Conference on World Wide Web, New York 2012,. s. 519–528.

[21] A. Guille i in., *Information Diffusion in Online Social Networks: A Survey*, „SIGMOD Record" 2013, nr 42, s. 17–28.

[22] S. Aral, D. Walker, *Identifying Influential and Susceptible Members of Social Networks*, „Science" 2012, nr 337, s. 337–341.

[23] S. Aral, *Identifying Social Influence: A Comment on Opinion Leadership and Social Contagion in New Product Diffusion*, „Marketing Science" 2011, nr 30, s. 1–7.

[24] Systemy rekomendacyjne automatycznie sugerują klientowi produkty i usługi dostosowane do jego potrzeb i zainteresowań; wykorzystują przy tym zebraną wiedzę o nim i o innych klientach.

[25] R. Iyengar, C. van den Bulte, T.W. Valente, *Opinion leadership and social contagion in new product*

Dyfuzja informacji w sieciach społecznościowych online zależy od siły związku pomiędzy użytkownikami sieci. Rozprzestrzenianie się informacji w sieciach o silnych związkach[26] różni się znacznie od dyfuzji w sieciach o związkach słabych[27] czy wręcz umownych[28]. W kontekście bezpieczeństwa narodowego istotne są zwłaszcza sieci o słabych i umownych związkach ze względu na łatwość prowadzenia wojny informacyjnej. Tego typu relacje występują na ogół na forach internetowych, które są klasycznym obszarem badań w zakresie analizy społeczności. Wszechstronny przegląd badań naukowych pod kątem analizy i eksploracji społeczności online (w tym szczególnie forów internetowych) zawiera opracowanie M. Morzego[29]. Istotnym nurtem badawczym jest identyfikacja wspomnianego wcześniej trollowania. Aktualny przegląd badań w tym zakresie oraz prezentację własnych, oryginalnych badań zawiera praca J. Chenga[30].

Ilościowa analiza mediów społecznościowych powinna być uzupełniona o analizę treści wpisów, m.in. z wykorzystaniem metod analiz lingwistycznych i eksplorację danych tekstowych (ang. *text miting*). Szczególnie popularna jest tzw. analiza wydźwięku (ang. *sentiment analysis*)[31], która na podstawie automatycznego przetwarzania zdań w języku naturalnym umożliwia określenie opinii autora na dany temat[32].

Podsumowanie

Metody analityczne stosowane do badania mediów społecznościowych są obecnie dość zaawansowane, czego przykładem jest m.in. monografia R. Zafaraniego[33]. Potencjał zastosowań biznesowych tego rodzaju mediów zaowocował powstaniem dziesiątków książek, poradników oraz komercyjnych narzędzi monitoringu i analizy mediów społecznościowych[34]. Natomiast niewiele jest ogólnodostępnych publikacji dotyczących analiz sieci społecznych online w szeroko rozumianej sferze bezpieczeństwa i obronności, które najczęściej ograniczają się do wykorzystania mediów społecznościo-

diffusion, „Marketing Science" 2011, nr 2, s. 195–212.

[26] Przykładem sieci społecznej online o silnych związkach jest Facebook, gdzie powiązania pomiędzy użytkownikami są oparte w większości przypadków na rzeczywiście istniejących znajomościach. Warunkiem istnienia silnych związków jest identyfikowanie użytkowników przez pryzmat rzeczywistych danych identyfikacyjnych.

[27] Przykładem słabych związków są specjalizowane fora internetowe, na których więzi są wyznaczone na zasadzie przynależności do danego forum, interakcji publicznych na forum, interakcji prywatnych za pośrednictwem poczty elektronicznej, sporadycznych spotkań w ramach zjazdów grup zainteresowań itp. Koniecznym warunkiem dla zaistnienia słabych związków jest identyfikowanie się przez używanie niezmiennego pseudonimu (nick) oraz umożliwienie kontaktu prywatnego.

[28] Przykładem związków umownych są ogólnodostępne fora internetowe, publiczne komentarze na portalach informacyjnych, na których w zdecydowanej większości przypadków jedyna relacja pomiędzy użytkownikami wynika z tego, że obie strony korzystają z tego samego forum. W takich sytuacjach tożsamość użytkowników jest zwykle całkowicie anonimowa.

[29] M. Morzy, *Analysis and Mining of Online Communities of Internet Forum Users*, w: *Data Mining: Foundations and Intelligent Paradigms*, D.E. Holmes, L.C. Jain (red.), seria: Intelligent Systems Reference Library 2012, t. 24.

[30] J. Cheng, C. Danescu-Niculescu-Mizil, J. Leskovec, *Antisocial Behavior in Online Discussion Communities*, arXiv:1504.00680, 2015.

[31] B. Pang, L. Lee, *Opinion mining and sentiment analysis*, „Journal Foundations and Trends in Information Retrieval" 2008, nr 2, s. 1–135.

[32] Na przykład: *tweet* na Twitterze czy *comment* na Facebooku.

[33] R. Zafarani, M.A. Abbasi, H. Liu, *Social Media Mining. An Introduction*, *Cambridge* 2014.

[34] Przykładowy ranking narzędzi analizy mediów społecznościowych: http://social-media-monitoring-review.toptenreviews.com/ [dostęp: 31 XII 2015].

wych w analizach wywiadowczych na podstawie ogólnodostępnych źródeł informacji (ang. *Open Source Intelligence*)[35].

W praktyce wykorzystanie metod ilościowych jest ograniczone, gdyż dostępne dane są najczęściej niekompletne i niskiej jakości. Dane rejestrowane w mediach społecznościowych odzwierciedlają wyłącznie faktyczną aktywność[36], poza analizą znajduje się natomiast niezarejestrowana działalność, jak np. przeglądanie profili innych użytkowników oraz czytanie wpisów. Przy uwzględnieniu tylko tych ograniczeń jest oczywiste, że wykorzystywanie analizy mediów społecznościowych do identyfikacji wojny informacyjnej powinno być ograniczone do wspierania analizy jakościowej przeprowadzanej przez odpowiednio wykwalifikowane zespoły analityczne[37].

Na zakończenie warto wspomnieć o udanych próbach wykorzystania mediów społecznościowych do rekrutacji członków islamistycznych ugrupowań terrorystycznych[38]. To zjawisko wymaga poważnej analizy. Aktualny stan badań nad stosowaniem metod analizy sieci społecznych w rozpoznaniu przestępczości zorganizowanej przedstawiono w dalszej części artykułu.

Wykorzystanie metod analizy sieci społecznych w rozpoznawaniu działalności zorganizowanych grup przestępczych

Analiza sieci społecznych umożliwia zgromadzenie istotnych, unikatowych informacji na temat organizacji przestępczych[39] – począwszy od rekrutacji członków po rozwój organizacji, przepływ informacji i rozprzestrzeniane przez nie idee. Zdobycie tego typu danych może skutecznie wspierać działania związane z wykrywaniem, śledzeniem i likwidowaniem działalności przestępczej.

Przegląd badań naukowych

Pierwsze poważne nawiązanie do analizy sieci społecznych pod kątem walki z przestępczością zorganizowaną zawiera monografia J. Arquilla z 2001 r.[40] Badania w tym zakresie zostały zainspirowane atakiem terrorystycznym z 11 września 2001 r.[41] Warto tu wspomnieć pracę V. Krebsa[42], który na podstawie dostępnych informacji stworzył mapę sieci powiązań Al-Kaidy. Ta praca w pełni odzwierciedla ówczesny stań badań ograniczający się do przestudiowania wybranych organizacji terrorystycznych na podstawie ogólnie dostępnych danych. Badania jakościowe były najczęściej uzupełniane o badania ilościowe, w których wykorzystywano metody analizy sieci społecznych. Dobrze

[35] F.Y. Wang i in., *Social computing: From social informatics to social intelligence*, „Intelligent Systems, IEEE" 2007, nr 22, s. 79–83.

[36] Na przykład: *retweet* na Twitterze, *like* na Facebooku.

[37] Taka metoda analizy danych jest jednym z pryncypiów firmy Palantir Technologies: *We believe in augmenting human intelligence, not replacing it* (*Jesteśmy przekonani, że ludzką inteligencję należy wspierać, a nie próbować ją zastępować* – tłum. aut.), która oferuje platformę wykorzystania analizy danych dla wsparcia pracy analityków wywiadu: https://www.palantir.com/about/ [dostęp: 31 XII 2015].

[38] http://www.cnn.com/2015/06/04/us/isis-social-media-recruits/ [dostęp: 31 XII 2015].

[39] W niniejszym artykule pojęcie organizacje przestępcze obejmuje przede wszystkim organizacje terrorystyczne, ale odnosi się także do innych zorganizowanych grup przestępczych, np. grup hackerskich.

[40] J. Arquilla, D. Ronfeldt, *Networks and Netwars*, Santa Monica 2001.

[41] Było to również silnie powiązane z zainteresowaniem środowiska naukowego gwałtownym wzrostem popularności sieci społecznych online, takich jak Myspace czy Facebook, które powstały odpowiednio w 2003 i 2004 r.

[42] V. Krebs, *Mapping Networks of Terrorist Cells*, „Connections" 2001, nr 24, s. 43–52.

opracowany przegląd badań jakościowych zawiera opracowanie S. Resslera[43]. W kolejnych latach opublikowano wiele prac zbiorowych przedstawiających aktualny stan badań w tej dziedzinie. Najważniejsze z nich to monografia N. Memona[44], M. Ranstropa[45], U. Wiila[46] i V.S. Subrahmaniana[47]. Tematyce analizy sieci organizacji terrorystycznych zostało poświęcone specjalne wydanie „Behavioral Sciences of Terrorism & Political Aggression", które ukazało się w 2013 r.[48]

Dzięki grantom przyznanym przez rząd Stanów Zjednoczonych było możliwe powstanie kilku grup badawczych zajmujących się wsparciem walki z terroryzmem. Grupa naukowa z Carnegie Mellon University[49] opracowywała środowisko badawcze Dynamic Network Analysis łączące tradycyjne metody analizy sieci społecznych z metodami wieloagentowymi i analizami lokalizacyjnymi[50]. W tym podejściu grupa terrorystyczna jest interpretowana jako system sieciowy ewoluujący w czasie. Na Uniwersytecie Arizona[51] zrealizowano projekt Dark Web, którego celem było badanie grup terrorystycznych z wykorzystaniem metod ilościowych i narzędzi sztucznej inteligencji[52]. W ramach tego projektu zrealizowano m.in. badania dotyczące analizy forów internetowych pod kątem zwolenników organizacji terrorystycznych[53].

Rozwój badań i przede wszystkim rozpowszechnienie ogólnodostepnych baz danych dotyczących przestępczości zorganizowanej zaowocował wieloma publikacjami w renomowanych czasopismach naukowych. Do najważniejszych artykułów (wyliczonych w kolejności chronologicznej opublikowania) można zaliczyć prace autorstwa: B.A. Jacksona[54], S. Koschade'a[55], R. Lindelaufa[56], S. Mahesha[57], N. Chaurasi[58], B.A. Desmarais'go[59] i R.M. Mediny[60].

---

[43] S. Ressler, *Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research*, „Homeland Security Affairs" 2006, t. 2.

[44] *Mathematical methods in counterterrorism*, N. Memon, J.D. Farley, D.L. Hicks, T. Rosenorn (red.), Wien–New York 2009.

[45] *Mapping terrorism research: State of the art, gaps and future direction*, M. Ranstorp (red.), b.m.w. 2007 (także: https://www.fhs.se/.../2007/mapping-terrorism-research.pdf – przyp. red.).

[46] *Counterterrorism and Open Source Intelligence*, U. Wiil (red.), seria: Lecture Notes in Social Networks, 2011.

[47] *Handbook of computational approaches to counterterrorism*, V.S. Subrahmanian (red.), b.m.w. 2013.

[48] S. Mullins, *Special issue: Applying social network analysis to terrorism*, „Behavioral Sciences of Terrorism & Political Aggression" 2013, nr 5, s. 67–175.

[49] Center for Computational Analysis of Social and Organizational Systems, http://www.casos.cs.cmu.edu/ [dostęp: 31 XII 2015].

[50] K.M. Carley, *Dynamic network analysis*, w: *Dynamic social network modeling and analysis: Workshop summary and papers*, R. Breiger, K.M. Carley, P. Pattison (red.), Washington 2003, s. 133–145.

[51] *Dark Web and Geo Political Web Research*, http://ai.arizona.edu/research/terror/ [dostęp: 31 XII 2015].

[52] H. Chen, *Dark Web. Exploring and Data Mining the Dark Side of the Web*, New York 2012.

[53] A. Abbasi, H. Chen, *Applying Authorship Analysis to Extremist-Group Web Forum Messages*, „Intelligent Systems, IEEE" 2005, nr 20, s. 67–75.

[54] B.A. Jackson, *Groups, networks, or movements: A command-and-control driven approach to classifying terrorist organizations and its application to Al Qaeda*, „Studies in Conflict &Terrorism" 2006, nr 29, s. 241–262.

[55] S. Koschade, *A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence*, „Studies in Conflict & Terrorism" 2006, nr 29, s. 559–575.

[56] R. Lindelauf, P. Borm, H. Hamers, *The influence of secrecy on the communication structure of covert networks*, „Social Networks" 2009, nr 31, s. 126–137.

[57] S. Mahesh, T.R. Mahesh, M. Vinayababu, *Using data mining techniques for detecting terror-related activities on the Web*, „Journal of Theoretical & Applied Information Technology" 2010, nr 16, 99–104.

[58] N. Chaurasia i in., *A survey on terrorist network mining: Current trends and opportunities*, „International Journal of Computer Science & Engineering Survey" 2012, nr 3, s. 59–66.

[59] B.A. Desmarais, S.J. Cranmer, *Forecasting the locational dynamics of transnational terrorism: A network analytic approach*, „Security Informatics" 2013, nr 2, s. 1–13.

[60] R.M. Medina, *Social network analysis: A case study of the Islamist terrorist network*, „Security Journal"

Jak już wspomniano, pierwsze badania organizacji przestępczych były ograniczone do klasycznej analizy ilościowej. Przykładowo w książce R. Gupty[61] omówiono praktyczne zastosowania analizy mediów społecznościowych w przypadku zagadnień dotyczących bezpieczeństwa, używając klasycznych metryk (jak: *centrality* L. Bonaciego i *betweenness* L. Freemana), które służyły identyfikacji wpływowych użytkowników Twittera. Rozwój badań w ostatnich latach zaowocował kilkoma zaawansowanymi publikacjami książkowymi, wśród których na szczególną uwagę zasługuje monografia S.F. Evertona[62], w praktyczny sposób przedstawiająca metody analiz sieciowych w badaniu zorganizowanych grup przestępczych. Aktualny przegląd badań w ramach omawianej tematyki jest zawarty w opracowaniu D. Knokego[63].

Podsumowanie

Przeprowadzanie zaprezentowanych badań naukowych jest ograniczone z jednego prozaicznego powodu. Dane wykorzystane w tych pracach pochodzą z publicznie dostępnych źródeł, co powoduje, że są one niekompletne. Pozytywne wyniki uzyskane mimo tego ograniczenia wskazują na potencjał metod analitycznych. W tym przypadku zastosowanie omówionych metod przez instytucje rządowe mające dostęp do informacji niejawnych wydaje się uzasadnione.

Drugim ważnym ograniczeniem dotyczącym zespołów akademickich jest ich pobieżna znajomość funkcjonowania organizacji przestępczych. Konsekwencją tej sytuacji są bardzo uproszczone analizy i brak odwołania do rzeczywistych problemów związanych ze ściganiem organizacji przestępczych. Prowadzenie wiarygodnych i użytecznych badań wymaga ich przeprowadzania w zespołach interdyscyplinarnych z udziałem ekspertów i praktyków.

Zakończenie

Przedstawiony stan wiedzy i badań na temat sieci społecznych online jest ograniczony wyłącznie do ogólnodostępnych, oficjalnie publikowanych badań naukowych. Zakres badań naukowych prowadzonych bezpośrednio na rzecz obronności i bezpieczeństwa wewnętrznego jest – z oczywistych powodów – utajniony. W Stanach Zjednoczonych ta klauzula tajności została złamana w 2013 r. przez Edwarda Snowdena[64]. Niektóre z wykradzionych przez niego dokumentów zostały udostępnione do publicznej wiadomości[65]. Ich analiza wskazuje na ogromne zainteresowanie National Security Agency tematyką omawianą w niniejszym artykule i na dojrzałość rozwiązań wykorzystywanych w praktyce. Należy jednocześnie podkreślić, że spektakularne sukcesy związane z wykorzystaniem analizy mediów społecznościowych w zastosowaniach biznesowych, takich jak zarządzanie relacjami z klientami, nie są zwykle publikowane. Nieujawnianie i ochrona rozwiązań analitycznych przed kopiowaniem przez konkurencję jest w biznesie naturalną metodą budowania przewagi konkurencyjnej opartej na innowacyjnych rozwiązaniach.

2014, nr 27, s. 97–121.

[61] R. Gupta, H. Brooks, *Using Social Media for Global Security*, Indianapolis 2013.

[62] S.F. Everton, *Disrupting dark networks*, Cambridge 2012.

[63] D. Knoke, *Emerging Trends in Social Network Analysis of Terrorism and Counterterrorism*, w: *Emerging Trends in the Social and Behavioral Sciences*, R. Scott, S. Kosslyn (red.), Hoboken 2015.

[64] E. Lucas, *The Snowden Operation: Inside the West's Greatest Intelligence Disaster*, b.m.w. 2014.

[65] https://firstlook.org/theintercept/documents/ [dostęp: 31 XII 2015].

Skala sukcesu praktycznych zastosowań analizy sieci społecznych online jest znacząca, a wyniki badań naukowych omówionych w artykule zasługują na uwagę ze strony służb odpowiedzialnych za bezpieczeństwo narodowe. W tym kontekście prowadzenie własnych prac badawczo-rozwojowych nad mediami społecznościowymi pod kątem bezpieczeństwa narodowego, ukierunkowanych na praktyczne zastosowania, jest wysoce uzasadnione.

Bibliografia:

1. Abbasi A., Chen H., *Applying Authorship Analysis to Extremist-Group Web Forum Messages*, „Intelligent Systems, IEEE" 2005, nr 20, s. 67–75.
2. Aral S., *Identifying Social Influence: A Comment on Opinion Leadership and Social Contagion in New Product Diffusion*, „Marketing Science" 2011, nr 30, s. 1–7.
3. Aral S., Walker D., *Identifying Influential and Susceptible Members of Social Networks*, „Science" 2012, nr 337, s. 337–341.
4. Arquilla J., Ronfeldt D., *Networks and Netwars*, Santa Monica 2001, RAND.
5. Baksy E. i in., *The role of social networks in information diffusion*, Proceedings of the 21 International Conference on World Wide Web, New York 2012, s. 519–528.
6. Boyd D.M., Ellison N.B., *Social network sites: Definition, history, and scholarship*, „Journal of Computer-Mediated Communication" 2007, nr 13, s. 210–230.
7. Brzeski R., *Wojna informacyjna – wojna nowej generacji*, Komorów 2014, Antyk.
8. Carley K.M., *Dynamic network analysis*, w: *Dynamic social network modeling and analysis: Workshop summary and papers,* R. Brieger, K.M. Carley, P. Pattison (red.), Washington 2003, b.w., s. 133–145.
9. Chaurasia N. i in., *A survey on terrorist network mining: Current trends and opportunities*, „International Journal of Computer Science & Engineering Survey" 2012, nr 3, s. 59–66.
10. Chen H., *Dark Web. Exploring and Data Mining the Dark Side of the Web*, New York 2012, Springer.
11. Cheng J., Danescu-Niculescu-Mizil C., Leskovec J., *Antisocial Behavior in Online Discussion Communities*, arXiv:1504.00680, 2015.
12. *Counterterrorism and Open Source Intelligence*, U. Wiil (red.), seria: Lecture Notes in Social Networks, b.m.w. 2011.
13. Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, seria: Punkt Widzenia, Warszawa 2014, Ośrodek Studiów Wschodnich.
14. Desmarais B.A., Cranmer S.J., *Forecasting the locational dynamics of transnational terrorism: A network analytic approach*, „Security Informatics" 2013, nr 2, s. 1–13.
15. Duggan P.M., *Strategic Development of Special Warfare in Cyberspace*, „Joint Force Quarterly" 2015, nr 4, s. 46–53.
16. Everton S.F., *Disrupting dark networks*, Cambridge 2012*,* Cambridge University.
17. Ghonim W., *Revolution 2.0: The Power of the People Is Greater Than the People in Power: A Memoir*, Boston–New York 2013, Mariner Books.
18. Gupta R., Brooks H., *Using Social Media for Global Security*, Indianapolis 2013, John WIley & Sons.
19. Guille A., Hacid H., Favre C., Zighed D.A., *Information Diffusion in Online Social Networks: A Survey*, „SIGMOD Record" 2013, nr 42, s. 17–28.

20. Franke U., *War by non-military means. Understanding Russian information warfare*, Stockholm 2015 (Report No FOI-R–4065–SE), Swedish Defence Research Agency.
21. *Handbook of computational approaches to counterterrorism*, V.S. Subrahmanian (red.), New York 2013, Springer.
22. Hughes A., Palen L., *Twitter adoption and use in mass convergence and emergency events*, „International Journal of Emergency Management" 2009, nr 6, s. 248–260.
23. Iyengar R., Bulte C. van den, Valente T.W., *Opinion leadership and social contagion in new product diffusion*, „Marketing Science" 2011, nr 2, s. 195–212.
24. Jackson B.A., *Groups, networks, or movements: A command-and-control driven approach to classifying terrorist organizations and its application to Al Qaeda*, „Studies in Conflict &Terrorism" 2006, nr 29, s. 241–262.
25. Jaitner M., Mattsson P.A., *Russian Information Warfare of 2014*, 7th International Conference on Cyber Conflict, NATO CCD COE Publications 2015, s. 29–52.
26. Kaplan A.M., Haenlein M., *Users of the world, unite! The challenges and opportunities of social media,* „Business Horizons" 2010, nr 53, s. 59–68.
27. Knoke D., *Emerging Trends in Social Network Analysis of Terrorism and Counterterrorism*, w: *Emerging Trends in the Social and Behavioral Sciences*, R. Scott, S. Kosslyn (red.), Hoboken 2015, John Wiley & Sons.
28. Koschade S., *A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence*, „Studies in Conflict & Terrorism" 2006, nr 29, s. 559–575.
29. Krebs V., *Mapping Networks of Terrorist Cells*, „Connections" 2001, nr 24, s. 43–52.
30. Lindelauf R., Borm P., Hamers H., *The influence of secrecy on the communication structure of covert networks*, „Social Networks" 2009, nr 31, s. 126–137.
31. Lucas E., *The Snowden Operation: Inside the West's Greatest Intelligence Disaster*, b.m.w. 2014, b.w.
32. Mahesh S., Mahesh T.R., Vinayababu M., *Using data mining techniques for detecting terror-related activities on the Web*, „Journal of Theoretical & Applied Information Technology" 2010, nr 16, 99–104.
33. *Mapping terrorism research: State of the art, gaps and future direction,* M. Ranstorp (red.), London 2007, Routledge.
34. *Mathematical methods in counterterrorism*, N. Memon i in. (red.), Wien–New York 2009, Springer.
35. Medina R.M., *Social network analysis: A case study of the Islamist terrorist network*, „Security Journal" 2014, nr 27, s. 97–121.
36. Morzy M., *Analysis and Mining of Online Communities of Internet Forum Users*, w: *Data Mining: Foundations and Intelligent Paradigms*, D.E. Holmes, L.C. Jain (red.), seria: Intelligent Systems Reference Library, t. 24, Berlin–Heidelberg 2012, Springer.
37. Mullins S., *Special issue: Applying social network analysis to terrorism*, „Behavioral Sciences of Terrorism & Political Aggression" 2013, nr 5, s. 67–175.
38. Pang B., Lee L., *Opinion mining and sentiment analysis*, „Journal Foundations and Trends in Information Retrieval" 2008, nr 2, s. 1–135.
39. Ressler S., *Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research*, „Homeland Security Affairs" 2006, t. 2.
40. Samadashvili S., *Muzzling the bear: Strategic Defense for Russia's Undeclared Information War on Europe*, Brussels 2015, Wilfried Martens Centre for European Studies.

41. Surma J., *The Role of Individual Behavior and Social Influence in Customer Relation Management*, w: *Handbook of Research on Managing and Influencing Consumer Behavior*, New York 2015, Springer, s. 385–396.
42. Wang F.Y. i in., *Social computing: From social informatics to social intelligence*, „Intelligent Systems, IEEE" 2007, nr 22, s. 79–83.
43. Wasserman S., Faust K., *Social Network Analysis. Methods and Applications*, Cambridge 1994, Cambridge University Press.
44. Zafarani R., Abbasi M.A., Liu H., *Social Media Mining. An Introduction*, Cambridge 2014, Cambridge University Press.

Abstrakt

Sieci społeczne online mają istotne znaczenie w funkcjonowaniu współczesnego społeczeństwa. Zastosowanie zaawansowanych metod analitycznych w ich badaniu może być wykorzystane do wsparcia zarządzania bezpieczeństwem narodowym w co najmniej dwóch aspektach. Po pierwsze umożliwia identyfikację wojny informacyjnej prowadzonej z wykorzystaniem mediów społecznościowych. Po drugie zaś udostępnia metody rozpoznania struktury i sposobów działania zorganizowanych grup przestępczych, takich jak na przykład organizacje terrorystyczne. Te dwa obszary zastosowań zostały omówione w odniesieniu do aktualnego stanu badań naukowych, ograniczeń w ich prowadzeniu oraz potencjalnego zastosowania tych badań w zakresie bezpieczeństwa narodowego.

Słowa kluczowe: sieci społeczne online, wojna informacyjna, rozpoznanie zorganizowanych grup przestępczych, metody ilościowe, eksploracja danych.

Abstract

Online social networks are essential dimension of modern society. Applying advanced analytical methods in social networks can be used to support of national security in at least two aspects. Firstly it allows identification information war, which is conducted with the use of social media. Secondly it provides methods for the recognition of the structure and methods of operation in organized criminal groups, such as terrorist organizations. These two areas of application are discussed in relation to the current state of art in scientific research, limitations, and potential applications in the national security.

Keywords: on-line social networks, information war, organized crime identification, quantitative methods, data mining.