Sosial mediada milli informasiya təhlükəsizliyinə təhdidlərin aşkarlanması üçün yanaşma

Ramiz Alıquliyev[1], Nərgiz İsmayılova[2]

[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

[1]r.aliguliyev@gmail.com; [2]nargiz.ni.21@gmail.com

***Xülasə* — Məqalədə sosial mediada dövlət əleyhinə və milli informasiya təhlükəsizliyinə qarşı təhdidlərin, kibercinayətkarlığın və terrorist qruplarının bədniyyətli fəaliyyətlərinin aşkarlanması üçün texnologiyalar analiz edilmiş və yanaşma təklif olunmuşdur.**

Açar sözlər — Big Data; sosial şəbəkə; terrorizm; informasiya təhlükəsizliyi

I. GİRİŞ

Müasir dövrdə kriminal qruplar təkcə real aləmdə deyil, həm də virtual mühitdə dövlət və cəmiyyət əleyhinə müxtəlif məqsədli (milli mentalitetə qarşı, mənəvi dəyərləri sarsıdan və s.) bədniyyətli fəaliyyətlərini həyata keçirirlər [1]. Kiberterrorizm bu gün milli təhlükəsizliyə ən böyük təhdidlərindən biridir. Hal-hazırda terrorist qrupların sosial şəbəkələr, e-mail və s. vasitələrlə ünsiyyət qurması mümkündür. Sosial şəbəkələrdən istifadənin artması müəyyən problemlər yaradır. Bu problemlərdən ən əsası informasiya təhlükəsizliyidir. Kiberterrorizmin aşkarlanmasında sosial şəbəkə analizinin xüsusi rolu vardır. Terrorizmə qarşı mübarizədə sosial şəbəkə analizinin əhəmiyyətinə 11 sentyabr 2001-ci ildəki hücumlardan əvvəl də diqqət yetirilirdi [2]. Bundan əlavə 2006-cı ildə ABŞ milli təhlükəsizlik təşkilatının dinləmə proqramları xəbərləri yayımlandıqda, terrorla mübarizə sahəsində sosial şəbəkə analizinin əhəmiyyəti New York Times məqaləsində də müzakirə olundu [3].

Bu məqalədə milli informasiya təhlükəsizliyinə qarşı təhdidlər, dövlət əleyhinə təxribatlar araşdırılmışdır. Sosial mediada terrorist qrupları aşkar etmək üçün Big Data analitika texnologiyaları imkanları analiz edilmişdir.

II. SOSİAL MEDİA VƏ MİLLİ TƏHLÜKƏSİZLİK

Sosial media İnternet texnologiyaları vasitəsilə insanlar arasında virtual sosial ünsiyyət yaratmaq və məlumatları paylaşma deməkdir. O, daha əlçatan və veb əsaslı texnologiyalardan istifadə etməklə ünsiyyəti interaktiv dialoqa çevirir. Sosial media vasitələrinə internet üzərindən yayımlanan informasiya saytları, sosial şəbəkələr, bloqlar, mikro bloqlar, ani ünsiyyət proqramları, forumlar daxildir. Sosial şəbəkələr bizim fiziki dünyamızın virtual formasıdır. Hal-hazırda terrorist qruplar sosial şəbəkələr, e-mail və s. vasitələrlə ünsiyyət qururlar. Aydındır ki, belə kommunikasiya vasitələrində ötürülən informasiya növləri arasında mətnlər üstünlük təşkil edirlər. Ona görə də, mümkün ola biləcək terror aktlarının qarşısının alınması və dövlətin təhlükəsizliyinin təmin olunması üçün virtual mühitdə, o cümlədən sosial mediada dövr edən mətnlərin analizi mühüm əhəmiyyət kəsb edir [4]. Hal-hazırda mətnlərdən nümunələri, açar sözləri və müvafiq məlumatları aşkar etmək üçün Big Data analitika texnologiyalarından (data mining, text mining və s.) istifadə olunur [5].

A. Şəbəkə analizi

Müasir sosial şəbəkə analizini araşdırarkən Stanley Milgramın apardığı təcrübələrə baxmaq olar [6]. 11 sentyabr 2001-ci il hücumundan sonra sosial şəbəkə ekspertləri terrorizmə qarşı mübarizədə şəbəkə metodologiyasının istifadəsinə daha çox üstünlük verməyə başladılar. Washington Post və Dallas Morning News kimi nəşrlər şəbəkə analizi haqqında məqalələr yazdılar [7]. Sosial şəbəkələrin dinamik təbiətini öyrənməyə kömək etmək, cinayət və ya terrorist şəbəkələri öyrənmək üçün bir çox modellər (agent-əsaslı modellər və s.) hazırlanmışdır.

B. Mətnlərin analizi

Mətnlərin analizi zamanı ilk öncə mətnlərin klassifikasiyasına baxılır. Əvvəlcə hansı sözlərin əhəmiyyətli olduğunu müəyyən etmək lazımdır. Daha sonra mətnə müəyyən olunmuş sözlərlə sorğu verilir. Məs: “cinayət”, “terror”, “girov” və s. [8]. Sorğunun nəticəsinə uyğun olaraq mətn “şübhəli” və ya “şübhəsiz” kateqoriyasına daxil olur.

Tutaq ki, hər hansı sosial şəbəkədə (Facebook, Twitter və s.) dövlətin sosial siyasətilə əlaqəli mətn verilmişdir. Şərhlərdə ifadə olunan fikirləri analiz etməklə bu mətni 3 əsas kateqoriyaya görə təsnifatlaşdırmaq olar: 1) Radikal fikirlərlə bağlı ifadələr – R kateqoriyası, 2) müdafiə məqsədli ifadələr – C kateqoriyası, 3) Neytral siyasi mövqeyə sahib olan və ya siyasi məzmunu olmayan bütün şərhlər – N kateqoriyası. Bundan əlavə müəyyən kateqoriyalara siyasi mənsubiyyəti göstərən sözlər lüğəti qurula bilər. Bu zaman yazılan şərhlər mətndə istifadə olunan sözlərə görə klassifikasiya olunur və müvafiq kateqoriyaya aid edilir [9].

DOI: 10.25045/NCInfoSec.2017.15

C. İstifadəçi analizi

İstifadəçi analizi – onlayn sosial şəbəkələrdə istifadəçi davranışlarının xarakterizə olunması və əlaqələrin qiymətləndirilməsidir. İnsanların bu günlərdə internetdə paylaşa biləcəkləri məlumatlara demək olar ki, məhdudiyyət yoxdur və sosial mediada məlumatların geniş və tez yayıldığını nəzərə alsaq, bu əslində potensial olaraq təhlükəlidir. Belə ki, insanlar öz şəxsi məlumatlarını çəkinmədən sosial şəbəkələrdə paylaşırlar. Bəzən bu məşhur olmaq üçün, bəzən də sadəcə diqqətsizlikdir [10]. Ona görə də istifadəçi analizi kiber təhlükəsizliyin tələb etdiyi müəyyən problemlərdən biridir. Burada saxta profillərin, gizli sosial şəbəkələrin aşkarlanması və analizi mühüm məsələlərdən biridir. Normal sosial şəbəkədə güclü əlaqələr şəbəkə üzvlərinin klasterizasiyasını həyata keçirir, lakin gizli şəbəkədə aktivləşmə tezliyi kiçik olduğundan güclü əlaqələr zəif əlaqə kimi görünə bilər. Şəbəkə nə qədər az aktivdirsə, onu aşkarlamaq o qədər çətindir [11].

D. Sosial media monitorinqi

Monitorinq şəbəkənin (proqramın və s.) məqsədinə çatmaq istiqamətində irəliləməsi və düzgün nəticələr almaq üçün məlumatların toplanması və analizinin sistemli prosesidir. Sosial medianın monitorinqi aşağıda qeyd olunan məsələlərin həllinə kömək edir.

- auditoriyanın maraqlarını nəzərə almaq, insanların istək və arzularını dəqiqliklə müəyyən etmək;
- insanlarla interaktiv əlaqə yaratmaq;
- auditoriyanın tələbatı olan məlumatları sosial media vasitəsilə yaymaq;
- qurumun gələcək fəaliyyətini analiz etmək [12].

Sosial mediada monitorinq zamanı ilkin olaraq informasiyalar izlənir, mətnlər analiz olunur, spam şərhlər təyin olunur. Növbəti addımlarda məntlərin müxtəlif xüsusiyyətlərinə görə daha ətraflı təhlil aparılır. Daha sonra isə vizualizasiya və yarana biləcək təhdidlərə qarşı tədbirlər görülür [13].

III. TƏKLİF OLUNAN YANAŞMA

Sosial mediada gizli sosial şəbəkələrin aşkarlanması dövlətin təhlükəsizliyinin təmin olunması və idarəetmənin yaxşılaşdırılmasında əsas amillərdən biridir. Hal-hazırda müxtəlif terror təşkilatları əlaqə yaratmaq üçün sosial medianın imkanlarından geniş istifadə edirlər və belə təşkilatlar münasibətlərini həmişə gizli saxlayırlar. Sosial media bu kimi məlumatları izləmək üçün analiz olunmalıdırlar. Bu problemləri nəzərə alaraq aşağıdakı yanaşmanı təklif edirik. Təklif etdiyimiz yanaşma 4 prosesdən ibarətdir.

1) Məlumatların toplanılması.

Məlumatların toplanılması prosesində Big Data texnologiyalarından istifadə oluna bilər. Bu zaman data mining texnologiyalarının imkanlarından sistemli şəkildə istifadə etmək lazımdır. Məlumatların toplanılması zamanı ortaya çıxan əsas problem mənbələrin etibarlılığı problemidir.

2) Məlumatların saxlanılması.

Hal-hazırda məlumatların saxlanılması üçün DAS (Direct-Attach Storage), NAS (Network Attached Storage), SAN (Storage Area Networks) və s. kimi texnologiyalardan istifadə olunur. Lakin böyük verilənlərə gəldikdə isə bu saxlama arxitekturalarının çatışmazlıqları və məhdudiyyətləri ortaya çıxır. Buna görə də saxlanma qurğuları böyük həcmli verilənlərin əlyetərliyini və operativ analizini təmin etmək imkanlarına malik olmalıdır.

3) Məlumatların emalı.

Məlumatların emalı 3 mərhələdən ibarətdir: məlumatların təmizlənməsi, inteqrasiyası və transformasiyası. Təmizləmə mərhələsində bütün etibarsız və lazımsız məlumatları aradan qaldırmaq lazımdır. Müxtəlif mənbələrdən paylanmış ortaq məlumatların təhlili üçün məlumatların inteqrasiyası aparılmalıdır. Bu halda məlumatların emalı effektiv şəkildə həyata keçirilə bilər. Məlumatların transformasiyası dedikdə, məlumatın emalı və analizi üçün uyğun formata çevrilməsi nəzərdə tutulur.

4) Məlumatların vizuallaşdırılması.

Şəbəkə analizində əsas məsələlərdən biri də nəticələrin təqdim olunması – vizuallaşdırılmasıdır. Böyük ölçüyə və həcmə malik böyük verilənlərin vizuallaşdırılması xüsusilə çətindir. Burada bir neçə problem ortaya çıxır.

- İstifadəçi ekranda görünən məlumatı azalda bilər, lakin bu da informasiya itkisinə səbəb olur (information loss)
- İstifadəçi məlumatları müşahidə edir, lakin göstərilən məlumat dəyişikliyinə reaksiya bildirə bilmir (high rate of image change)
- Daha az sürətdə daha çox məhsuldarlıq tələb olunur. Bu da statistik vizuallaşdırmada çətinliklər yaradır (high performance requirements) və s.

Bu problemlərin aradan qaldırılması üçün yeni üsulların və texnologiyaların işlənməsi lazımdır.

NƏTİCƏ

Məlumdur ki, Big Data texnologiyaları mətnlərin analizində və identifikasiyasında çox böyük imkanlara malikdir. İnsan hüquqlarını və ifadə azadlığını pozmadan sosial media verilənlərinin monitorinqi və analizi cəmiyyətin nəbzini tutmağa, fikrini proqnozlaşdırmağa imkan verir. Sosial media analitikası meydana çıxan təhdidləri vaxtında aşkarlamağa və əks-tədbirlər həyata keçirməyə şərait yaradır. Lakin bunlar hələ də terror təşkilatlarının tamamilə aşkarlanması üçün kifayət deyil. Bu problemlərin həlli üçün yeni üsullar, yeni texnologiyalar lazımdır. Bununla yanaşı, terrorist şəbəkələrinin iştirakçıları necə cəlb etdiyini və insanların terror şəbəkəsinə qoşulmaq istəklərini anlamaq da vacibdir.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – **Qrant №EİF – KETPL – 2 – 2015 – 1 (25) - 56/05/1**

ƏDƏBİYYAT

[1] R.M. Alıquliyev, G.Y. Niftəliyeva “E-dövlət mühitində terrorizmlə əlaqəli mətnlərin aşkarlanması metodu,” İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015, s.111-115.

[2] S. Ressley “Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research,” Homeland Security Affairs, 2006. Vol. II, № 2. pp.1-9.

[3] K. Patrick, “Can Network Theory Thwart Terrorists?,” New York Times, March 12, 2006.

[4] Алыгулиев Р.М. “Роль технологии интеллектуального анализа текстов в обеспечении национальной безопасности”, Проблемы Информационных Технологий, 2013, № 1, с.38-43.

[5] C.C Aggarwal., C.X. Zhai. “Mining text data,” 2012, 524 p.

[6] St. Milgram, “The Small World Problem,” Psychology Today, 1967, pp. 60-67.

[7] J. Garreau, “Disconnect the Dots,” Washington Post, September 17, 2001

[8] D. Choi, B. Ko , H. Kim , P. Kim. “Text analysis for detecting terrorism-related articles on the web,” Journal of Network and Computer Applications/ 2014. pp.16-21.

[9] D. Gritzalis, M. Kandias, V. Stavrou, L. Mitrou. “History of Information: The case of Privacy and Security in Social Media,” Proc. of the History of Information Conference, 2014, pp. 283-310

[10] D. Hiatt, B.Choi Young, “Role of Security in Social Networking” International Journal of Advanced Computer Science and Applications, vol. 7, №. 2, 2016, pp.12-15.

[11] R.M.Əliquliyev, Y.N.İmamverdiyev, F.C. Abdullayeva. Sosial şəbəkələr, Bakı, 2010, s. 278.

[12] R.M. Əliquliyev, S.R. Ağayeva, “Internet-media resurslarının monitorinqi: müasir vəziyyətləri, problemləri və inkişaf perspektivləri. İnformasiya cəmiyyəti problemləri, 2016, №1, s. 63 – 70.

[13] M.D. Sykora, T.W. Jackson, A. O'Brien. “National security and social media monitoring: a presentation of the emotive and related systems” Intelligence and Security Informatics Conference (EISIC), 2013, pp.1-5.

APPROACH TO THE DETECTION OF THREATS TO NATIONAL INFORMATION SECURITY IN SOCIAL NETWORKS

Ramiz Aliguliyev[1], Nargiz Ismayilova[2]
[1,2]Institute of Information Technology of ANAS,
Baku, Azerbaijan
[1]r.aliguliyev@gmail.com; [2]nargiz.ni.21@gmail.com

Abstract – The article analyzes technologies for detecting threats to national information security, cybercrime and terrorist groups in social networks, and an approach is suggested.

Keywords – big Data; social network; terrorism; information security