Vikipediya Mühitində İnformasiya Müharibəsi Təzahürlərinin Aşkarlanması və Rəqəmsal Ekspertizası

İradə Ələkbərova
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
airada.09@gmail.com

***Xülasə*— Dünyanın ən böyük kollektiv bilik resursu olan Vikipediya, son illərdə informasiya əməliyyatlarının və hibrid müharibələrin aktiv poliqonuna çevrilmişdir. Tədqiqat çərçivəsində süni intellekt modellərinə əsaslanan proaktiv rəqəmsal ekspertiza modeli təklif edilmişdir. Məqalədə rəqəmsal sübutların toplanması, məlumatın tamlığının qorunması və istifadəçi davranışının analizi əsasında proaktiv müdafiə sisteminin qurulması mexanizmləri elmi və nəzəri baxımdan əsaslandırılır. Təklif olunan yeni yanaşma rəqəmsal ekosistemlərdə informasiya təhlükəsizliyinin təmini və dövlətin rəqəmsal suverenliyinin qorunması üçün əhəmiyyətli potensiala malikdir.**

Açar sözlər*— *Vikipediya; informasiya müharibəsi; rəqəmsal ekspertiza; vandalizm.

I. GİRİŞ

Dünyada ildən-ilə daha da mürəkkəbləşən sosial-siyasi proseslər dövlətlərin öz milli maraqlarını və kibertəhlükəsizliklərini qorumaq üçün daha müasir texnologiyalardan istifadəni zəruri etmiş, informasiya təhlükəsizliyi və kibersuverenlik konsepsiyalarını aktuallaşdırmışdır [1]. Süni intellekt, böyük verilənlər (big data) və hibrid təhdidlərin artması şəraitində dövlətin öz rəqəmsal sərhədlərini qorumaq milli təhlükəsizliyin ən mühüm prioritetinə çevrilmişdir. Bu gün dövlətlərarası rəqabət ənənəvi döyüş meydanlarından qlobal rəqəmsal məkana keçmiş, İnternet "hibrid müharibə" adlanan yeni qarşıdurma formasının aparıcı alətinə çevrilmişdir [2].

İnformasiya müharibəsi həm dövlət, həm də cəmiyyət üçün ciddi təhlükə yaradan informasiya əməliyyatı olmaqla [3] qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi, hərbi potensialını ələ keçirmək, ictimai şüura təsir göstərməklə insanların davranışlarını dəyişmək və nəzarətdə saxlamaq uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir [3, 4].

Siyasi, iqtisadi və informasiya vasitələrinin kombinasiyasından ibarət olan informasiya müharibəsi strateji resurslar üzərində nəzarəti təmin etmək və ictimai münasibətlərə təsir göstərmək baxımından müxtəlif informasiya əməliyyatlarını özündə birləşdirir [5]. Bu baxımdan rəqəmsal texnologiyalar üzərindən dövlətin informasiya təhlükəsizliyinə və cəmiyyətin sabitliyinə təhdid yaradan informasiya müharibəsi konsepsiyası informasiya qarşıdurması, elektron müharibə, dezinformasiya və informasiya hücumu kimi informasiya əməliyyatları ilə daha təhlükəli hal almaqdadır İnformasiya müharibəsi texnologiyalarına dayanıqlılıq və öz kibertəhlükəsizliyini təmin etmək hər bir dövlətin əsas strateji vəzifəsidir.

Vikipediya müasir dövrdə təkcə bilik mənbəyi deyil, həm də psixoloji əməliyyatların və informasiya qarşıdurmaları üçün bir platformadır. Açıq redaktə prinsipi və qlobal etibarlılığı Vikipediya mühitini müxtəlif dövlətlər, kəşfiyyat xidmətləri və siyasi qruplar üçün manipulyasiya alətinə, dövlətlərin, siyasi qrupların və maraqlı tərəflərin apardığı informasiya müharibəsi meydanına çevirmişdir.

Vikipediya istifadəçiləri və redaktorlar viki-mühitdə dezinformasiyanın yayılması, mühüm tarixi faktların silinməsi və ya dəyişdirilməsi, aktiv istifadəçilərə qarşı mütəşəkkil hücumları və onların viki-mühitdən uzaqlaşdırılması kimi informasiya müharibəsi təzahürlərini dərhal tanımaqda çətinlik çəkirlər. Rəqəmsal ekspertiza (Digital Forensics və ya Computer Forensics) modelləri bu subyektiv qiymətləndirməni obyektiv riyazi meyarlarla əvəz edərək, informasiya əməliyyatlarını alqoritmik ekspertiza ilə aşkar etməyə imkan verir [6].

Tədqiqatın obyekti müasir informasiya müharibələri şəraitində Vikipediya platforması, tədqiqatın predmeti isə, informasiya müharibəsi texnologiyalarına qarşı rəqəmsal ekspertizadan effektiv istifadə üçün metodun işlənməsidir.

Tədqiqatın məqsədi müasir informasiya müharibələri təhdidlərini analiz etməklə Vikipediyada aparılan informasiya müharibəsi təzahürlərini aşkarlamaq üçün rəqəmsal ekspertiza modelini işləyib hazırlamaqdır. Bu məqsədlə məqalədə aşağıdakı məsələlərə baxılır:

- İctimai rəyin formallaşmasında Vikipediyanın rolu.
- Vikipediya mühitində informasiya müharibəsi təzahürləri.
- Vikipediya mühitində rəqəmsal ekspertizanın mərhələləri.
- Vikipediya mühitində rəqəmsal ekspertiza modelinin struktur sxemi.

II. İCTİMAİ RƏYİN FORMALAŞMASINDA VİKİPEDİYANIN ROLU

Dövlətin milli təhlükəsizliyinin təmin olunması artıq təkcə fiziki sərhədlərin qorunması ilə deyil, həm də öz milli informasiya resurslarının qorunması, virtual məkanda müstəqil

DOI: 10.25045/forensic.gov.2026.03

qərarvermə və özünü müdafiə imkanlarının formalaşdırılması ilə ölçülür [7]. Belə bir şəraitdə "rəqəmsal kriminalistika" və "rəqəmsal ekspertiza" anlayışı dövlətin informasiya təhlükəsizliyini və müstəqilliyini təmin edən fundamental strateji komponentlər kimi çıxış edir [8].

Vikipediya da daxil olmaqla virtual sosial media platformaları dezinformasiyaların yayılması, ictimai rəyin formalaşdırılması və cəmiyyətdə etiraz meyillərinin gücləndirilməsi üçün effektiv vasitəyə çevrilmişdir. Vikipediya, dünyanın ən böyük açıq ensiklopediyası olaraq, axtarış sistemlərinin (Google, Yandex və s.) əsas məlumat mənbəyidir. Bu səbəbdən, dövlətlər, xalqlar, tarixi şəxslər və hadisələr haqqında formalaşan beynəlxalq rəylər birbaşa Vikipediyadakı ensiklopedik məqalələrdə toplanmış informasiya ilə əlaqəlidir. Vikipediya sadəcə bir ensiklopediya deyil, həm də rəqəmsal diplomatiya alətidir, müxtəlif ölkələrin milli informasiya təhlükəsizliyinin tərkib hissələrindən biridir [9]. İstifadəçilər hər hansı mövzu haqqında ilk məlumatı buradan alır, ChatGPT və Gemini kimi süni intellekt (Sİ) modelləri əsas məlumat bazası kimi Vikipediyadan istifadə edirlər.

Wikidata və DBpedia kimi strukturlaşdırılmış bazalar hərbi müdaxilələrin ən geniş məlumat massivini təqdim edir. Lakin bu məlumatların 'həqiqət mənbəyi' (single source of truth) kimi istifadəsi onların manipulyasiyalardan azad olmasını tələb edir. Rəqəmsal Ekspertiza bu böyük verilənlər (Big Data) bazasının hərbi-strateji məqsədlər üçün təhlükəsizliyini və obyektivliyini təmin edən güclü mexanizmdir [10].

Ayda 1 milyarddan çox istifadəçi tərəfindən ziyarət olunan bu platforma, informasiya əməliyyatlarının əsas hədəfinə çevrilmişdir. Virtual mühitdə ən nəhəng informasiya mənbəyi olan Vikipediyada baş verən informasiya qarşıdurmaları, onları yaradan səbəblər və bu əməliyyatlarda iştirak edən gizli sosial şəbəkələrin aşkarlanması kimi məsələlər bu gün də öz aktuallığını saxlamaqdadır. Bu məsələlərin həllində rəqəmsal kriminalistika və rəqəmsal ekspertiza kimi informasiya əməliyyatlarının xüsusi yeri vardır.

Rəqəmsal ekspertiza sübutların necə toplandığını və işləndiyini izləmək üçün əməliyyatlar ardıcıllığını və prosesləri izləyir, sübutların dəyişdirilməsinin qarşısını alır. Nəticədə, rəqəmsal ekspertizadan əldə edilən sübutlar informasiya müharibəsi və qarşıdurmalarında iştirak edən tərəflərin məqsədlərini anlamaq, gizli sosial şəbəkələri aşkarlamaq və nəhayət baş verən insidentlərin qarşısını almaq üçün istifadə edilə bilər.

Vikipediya müxtəlif tipli informasiyanın toplanması, daima yenilənməsi və ya dəyişdirilməsi bir tədqiqat obyekti kimi analitikləri cəlb etməkdədir. İlk növbədə Vikipediyanın cəmiyyətin bilik daşıyıcılarını özünə cəlb etməsi və insanların öz biliklərini, vaxtlarını təmənnasız olaraq dünya ictimaiyyətinə bağışlamaq istəməsi mütəxəssislərin diqqətini cəlb edir.

Vikipediyanın yalnız ensiklopediya deyil, həm də nəhəng sosial şəbəkə olması bu virtual layihədə müxtəlif qruplaşmaların, informasiya qarşıdurmalarının yaranmasına səbəb olmuşdur. Ənənəvi sosial şəbəkələrdən fərqli olaraq Vikipediya kollektiv bilik bazasının təşkilində mühüm rol oynayır. Bu səbəbdən Vikipediya müxtəlif tipli tədqiqatlar üçün, əsasən də cəmiyyətdə baş verən proseslərin öyrənilməsində çox əlverişli mühitdir.

Axtarış sistemləri və Sİ platformaları Vikipediyanı "mütləq həqiqət" kimi qəbul etdiyi üçün, Vikipediyaya edilən bir hücum eyni zamanda bütün internet ekosisteminə təsir etməklə [11] viki-mühitdə informasiya müharibəsi təzahürlərinin aşkarlanması üçün rəqəmsal ekspertiza modellərindən istifadəni zəruri edir.

III. VİKİPEDİYA MÜHİTİNDƏ İNFORMASİYA MÜHARİBƏSİ TƏZAHÜRLƏRİ

A. Milli kibertəhlükəsizlik problemləri

Milli kibertəhlükəsizliyə yönələn təhdidlər müasir dövrdə dövlətin suverenliyi və ictimai sabitliyi üçün ən ciddi risk faktorlarından birinə çevrilmişdir. Bu təhdidlər təkcə kritik infrastruktur obyektlərinə (enerji sistemləri, maliyyə şəbəkələri, hərbi rabitə) edilən kiber-hücumlarla məhdudlaşmır, həm də dövlətin rəqəmsal məlumat bazalarına sızılması, dövlət sirri təşkil edən informasiyaların oğurlanması və hədəflənmiş kiber-casusluq fəaliyyətlərini əhatə edir. Eyni zamanda, virtual məkanda aparılan koordinasiyalı dezinformasiya kampaniyaları və milli mənəvi dəyərlərə qarşı yönəlmiş sistemli informasiya əməliyyatları cəmiyyətdə daxili parçalanma yaratmaq məqsədi güdür ki, bu da milli təhlükəsizlik arxitekturasında "rəqəmsal sərhədlərin" qorunmasını fiziki sərhədlər qədər vacib edir.

Dövlətin milli təhlükəsizliyi həm də onun öz tarixi, coğrafiyası və siyasi reallıqları haqqında məlumatın dürüstlüyünə nəzarət etmək qabiliyyətidir. Vikipediyada dövlət sərhədlərinin təhrif edilməsi, işğal faktlarının ört-basdır edilməsi və ya milli qəhrəmanların nüfuzdan salınması birbaşa informasiya suverenliyinə qarşı təhdiddir. Bu, dövlətin rəqəmsal məkanda öz "həqiqətini" qorumaq imkanlarını zəiflədir.

B. Vikipediyada informasiya müharibəsi

Vikipediyada informasiya müharibəsi ilk olaraq "düzgün ensiklopedik məqalə" prinsipinə hücumdur və bu hücumun qarşısını almaq üçün məqalələrin redaktə tarixçəsini, redaktorların IP ünvanlarını və mənbələrin etibarlılığını analiz edərək məlumatın saflığını qorumaq ilkin şərtdir. Bu məsələlərin həllində isə Rəqəmsal ekspertiza mühüm rol oynayır:

İstifadəçilərinin müxtəlif sahə mütəxəssislərindən təşkil olunması və fərqli düşüncə, siyasi baxış və ideyalar daşıması Vikipediyada səngiməyən informasiya qarşıdurmalarının və redaktə müharibələrinin baş verməsinin əsas səbəbidir. Siyasi və ya ideoloji maraqlar tədricən Vikipediyanın rəqəmsal strukturuna (məqalələrin daxilinə) sızdırılır və orada "tarixi həqiqət" formatını alır. Əgər fərqli tərəflər arasında neytral monitorinq aləti və ya ciddi fakt-yoxlama alqoritmi yoxdursa, onların fikirlərinin obyektiv bilikdə birləşməsi mümkün deyil [12]. Əksinə, rəqəmsal mühit bu münaqişəni daha da mürəkkəbləşdirəcək. İnformasiya texnologiyalarının, əsasən də Sİ-in məhsulları olan Deep feyk və s. alətlərindən istifadə nəticəsində Vikipediya da daxil olmaqla sosial media platformalarında (Facebook, Twitter, YouTube və s.) müşahidə olunan informasiya müharibəsi və informasiya qarşıdurmaları daha mürəkkəb və təhlükəli formalar almaqdadır.

Araşdırmalar nəticəsində aşağıdakı informasiya müharibəsi təzahürləri müəyyən olunmuşdur:

- *Dezinformasiya* (təhrif olunmuş informasiya). İnformasiyanın yalan məlumatla əvəz edilməsi, faktların təhrif edilməsi və mənbələrin saxtalaşdırılması nəticəsində cəmiyyətdə hər-hansı hadisəyə və ya şəxsə qarşı rəyin dəyişdirilməsi.
- *Hesabların ələ keçirilməsi*. Klassik kiber-hücum metodları ilə istifadəçilərin şəxsi hesablarının oğurlanması.
- *Vandalizm*. Aşkar şəkildə saxta və ya təhqiramiz məlumatın yerləşdirilməsi (ən asan aşkar edilən növ). Qarşı tərəfin daxil etdiyi məlumatların Vikipediya standartlarına uyğun gəlmədiyi bəhanəsi ilə və ya heç bir səbəb göstərmədən silinməsi.
- *Gizli neytrallıq pozuntusu*. "Neytral baxış bucağı" (NPOV) prinsipinin incə şəkildə pozulması, emosional yüklü epitetlərin əlavə edilməsi.
- *Mənbə manipulyasiyası*. Etibarsız və ya qərəzli mənbələrə istinad edərək yanlış məlumatın leqallaşdırılması.
- *Saxta istifadəçi hesablarından istifadə (Sockpuppeting)*. Bir şəxs tərəfindən idarə olunan çoxsaylı hesablar vasitəsilə süni konsensus yaratmaq cəhdi. Saxta məlumatları təbliğ etmək üçün saxta ekspert profillərinin yaradılması süni nüfuzun təbliğində də geniş yer tutur.

Sadalanan informasiya müharibəsi təzahürlər göstərir ki, Vikipediya artıq sadəcə kollektiv bilik resursu deyil, həm də dövlətlərarası geopolitik rəqabətin rəqəmsal cəbhə xəttidir. İnformasiya əməliyyatlarının hədəfi olan məqalələr çox vaxt milli kimlik, ərazi bütövlüyü və tarixi irslə bağlı olduğu üçün, bu sahədə aparılan rəqəmsal ekspertiza həm də milli təhlükəsizlik ekspertizası xarakteri daşıyır.

Rəqəmsal sübutların toplanması və sistemli analizi nəticəsində əldə olunan "gizli biliklər", dezinformasiya axınlarına qarşı strateji dözümlülüyü artırmaq və virtual məkanda dövlətin "informasiya suverenliyini" təmin etmək üçün vacib informasiyadır. Bu mürəkkəbləşmə şəraitində rəqəmsal ekspertiza təkcə statik məlumatların yoxlanılması ilə kifayətlənmir, həm də dinamik alqoritmik monitorinq mexanizmlərini tətbiq edir.

IV. VİKİPEDİYA MÜHİTİNDƏ RƏQƏMSAL EKSPERTİZANIN MƏRHƏLƏLƏRİ

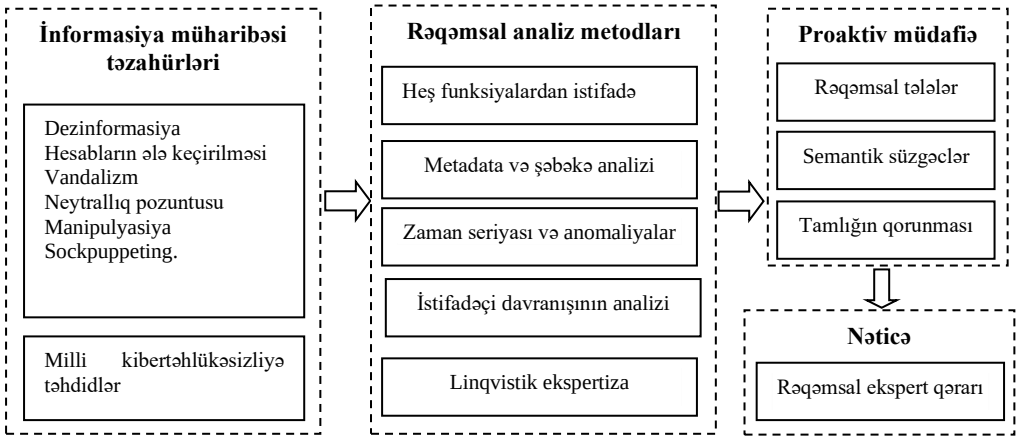
A. Rəqəmsal ekspertiza nədir?

Rəqəmsal ekspertiza, rəqəmsal cihazlarda (kompüterlər, smartfonlar, serverlər, bulud yaddaşları və s.) saxlanılan, ötürülən və ya yaradılan məlumatların hüquqi və ya texniki sübut kimi istifadə edilməsi üçün toplanması, qorunması, analizi və hesabatlaşdırılması prosesidir. Həmçinin, informasiya müharibəsi və kiber-təhlükəsizlik kontekstində rəqəmsal ekspertiza sadəcə "fayl bərpası" deyil, həm də məlumatın mənşəyinin və tamlığının (data Integrity) elmi metodlarla sübut edilməsidir.

Redaktor davranışlarının "rəqəmsal barmaq izi" (digital fingerprinting) analizi vasitəsilə mütəşəkkil qrupların gizli fəaliyyət trayektoriyası müəyyən edilir. Xüsusilə, neyron şəbəkələrinə əsaslanan proqnozlaşdırma modelləri redaktə tezliyi və məzmun dəyişikliyi arasındakı qeyri-xətti əlaqələri aşkar edərək, hələ baş verməkdə olan informasiya hücumlarını erkən mərhələdə lokallaşdırmağa imkan verir. Bu, kiber-məkanda dövlət maraqlarının müdafiəsi üçün proaktiv ekspertiza qatının yaradılması deməkdir.

B. Vikipediya mühitində rəqəmsal ekspertiza prosesi

Vikipediyada informasiya müharibəsi artıq sadə "copy-paste" mərhələsindən çıxıb. İndi Sİ botları vasitəsilə mütəşəkkil şəkildə məqalələr manipulyasiya edilir. Rəqəmsal ekspertiza modelləri, Vikipediya mühitində informasiya müharibəsi təzahürlərini "kiber-cinayət" hadisəsi kimi qəbul edir. Şəkil 1-də Vikipediya mühitində informasiya müharibəsi təzahürlərinin aşkarlanması üçün rəqəmsal ekspertiza modelinin struktur sxemi verilmişdir.



Şəkil 1. Vikipediya mühitində rəqəmsal ekspertiza modelinin struktur sxemi.

Rəqəmsal ekspertiza beynəlxalq standartlara (məsələn, ISO/IEC 27037) uyğun olaraq 3 əsas mərhələdən keçməlidir:

1. Elektron sübutların müəyyən edilməsi. Burada ən kritik qayda verilənlərin toplanması və etibarlı saxlanmasıdır.
2. Rəqəmsal analiz metodları. Bu mərhələyə Sİ modelləri daxil olur ki, onlar informasiya müharibəsi təzahürlərini avtomatik aşkar edir. Bu mərhələ aşağıdakı spesifik sahələrə bölünür:

- Heş funksiyalardan istifadə olunmaqla orijinal verilənlərin dəyişməz qalmasını təmin etmək mümkündür. Əgər nüsxənin (məqalənin) heş qiyməti orijinal ilə eyni deyilsə, o, hüquqi sübut kimi qəbul edilmir.
- Metaverilənlər (Metadata) analizi. Redaktənin hansı IP ünvanından, hansı saat qurşağında və hansı cihazla edildiyinin analizi. Bu, "koordinasiyalı hücumları" ifşa etməyə kömək edir.
- Şəbəkə ekspertizası. Redaktorlar arasındakı gizli əlaqələri və kənar resurslardan (məsələn, saxta xəbər saytlarından) gələn trafikin intensivliyini ölçür.
- Zaman seriyası və anomaliyaların analizi. Rəqəmsal ekspertiza və analiz blokunun bu bölməsi, klassik metodları (məsələn, tək bir redaktənin yoxlanılması) kənara qoyaraq, redaktorun davranışının zaman oxu üzərindəki trayektoriyasını analiz edir. Bu, informasiya müharibəsinin gizli fazalarını dəqiq şəkildə identifikasiya etməyə imkan verir.
- İstifadəçi davranışının analizi (User Behavior Analytics). İstifadəçi profilini öyrənən, onu izləyən və anomal davranış anında onu bloklayan sistemdir. İstifadəçinin (və ya botun) yazı sürəti, seçdiyi sözlər və redaktə vaxtları Sİ (LSTM, RNN və s.) vasitəsilə izlənilir. "Hücum ehtimalı" aşkarlandıqda redaktə prosesi avtomatik dayandırılır.
- Linqvistik ekspertiza. Mətnin yazılma üslubunu analiz edərək, fərqli profillər arxasında eyni şəxsin (və ya botun) dayandığını müəyyən etmək.

3. Tapılan sübutların sənədləşdirilməsi və proaktiv müdafiə strategiyasının işlənməsi. Proaktiv müdafiədə sistem keçmiş məlumat zəncirinə əsaslanaraq gələcəkdə manipulyasiyanın hansı saatlarda və hansı miqyasda baş verə biləcəyini öncədən proqnozlaşdırır.

Müasir informasiya qarşıdurmaları fonunda rəqəmsal ekspertiza təkcə insidentdən sonrakı (post-mortem) analizlə kifayətlənməməli, həm də dinamik müdafiə strategiyasını işləməlidir. Bu yanaşma, viki-mühitdə manipulyasiya cəhdləri başladığı andan etibarən sistemin müdafiə parametrlərini dəyişərək hücum edən tərəfin (aktorun) işini çətinləşdirir. Beləliklə, rəqəmsal ekspertiza sadəcə sübut toplayan mexanizmdən, informasiya hücumlarının və qarşıdurmaların qarşısını alan aktiv müdafiə alətinə çevrilir.

C. Vikipediyada proaktiv müdafiə vasitələri

Vikipediyada informasiya müharibəsi və rəqəmsal ekspertiza kontekstində proaktiv müdafiə, informasiya hücumu baş verdiyi anda onun təsirini minimuma endirmək əməliyyatıdır. Proaktiv müdafiə vasitələri bunlar ola bilər:

1 Rəqəmsal tələlər (Honeypots). İnformasiya müharibəsi aktorlarını və botları aldatmaq üçün yaradılan saxta hədəflərdir (ensiklopedik məqalələr). İstifadəçi bu "tələ" məqalələrə müdaxilə etdiyi anda onun IP ünvanları və koordinasiya mərkəzləri qeydə alınır.

2 Semantik süzgəclər (Semantic Firewall/Semantic filters). Mətnin mənasını və emosional yükünü analiz edən "ağıllı" süzgəclərdir. Bu vasitə mətn daxilindəki gizli neytrallıq pozuntularını, təhqiramiz və ya dezinformasiya xarakterli cümlə strukturlarını aşkarlayır.

3 Blokçeyn əsasında tamlığın qorunması (Blockchain-based Integrity). Məqalələrin və mənbələrin tamlığını qorumaq üçün mərkəzləşdirilməmiş qeydiyyat sistemlərindən istifadə. Dövlət əhəmiyyətli məqalələrin hər bir redaktəsinin heş (hash) dəyəri blokçeyn şəbəkəsində yadda saxlanılır. Hər hansı qeyri-qanuni və ya gizli verilənlər bazası səviyyəsində müdaxilə olduqda, sistem avtomatik olaraq orijinal versiya ilə uyğunsuzluğu aşkar edir və real-vaxt rejimində bərpa (self-healing) prosesini başladır.

Sİ anomaliyaları və informasiya müharibəsi təzahürlərini yüksək dəqiqliklə aşkar etsə də, yekun hüquqi və strateji qərarın qəbulu mütəxəssis-ekspertin səlahiyyətində qalmalıdır. Bu səbəbdən, təklif olunan modeldə proaktiv müdafiə mərhələsindən dərhal sonra "Rəqəmsal ekspert qərarı" blokunun yer alması strateji əhəmiyyət kəsb edir. Belə bir struktur sistemin tam avtonom olmadığını, əksinə, insan zəkası tərəfindən idarə və audit olunduğunu nümayiş etdirir. Eyni zamanda, bu yanaşma Sİ modellərində rast gəlinən alqoritmik qərəzlilik (algorithmic bias) probleminin qarşısını alır və əldə olunan rəqəmsal sübutların hüquqi legitimliyini təmin edir.

D. Vikipediyada süni intellekt əsaslı ekspertiza

Vikipediyadakı gizli informasiya əməliyyatlarını və bu əməliyyatlarda iştirak edən gizli sosial şəbəkələri aşkarlamaq üçün texniki bazadır. Vikipediya kimi nəhəng platformalarda informasiya müharibəsi təzahürlərini aşkar etmək üçün Sİ texnologiyaları ilə işləmək və rəqəmsal ekspertiza (digital forensics) bacarıqlarına malik yüksək ixtisaslı mütəxəssislər lazımdır.

TABLE I. ƏNƏNƏVİ RƏQƏMSAL KRİMİNALİSTİKA VƏ TƏKLİF OLUNAN EKSPERTİZA MODELİNİN MÜQAYİSƏSİ

Xüsusiyyətlər	**Ənənəvi kriminalistika**	**Ekspertiza modeli**
Reaksiya müddəti	İnsident baş verdikdən sonra	Real-vaxt rejimində və önləyici
Analiz obyekti	Statik fayllar və loqlar	Dinamik istifadəçi davranışı və kontent
Aşkarlama metodu	Qaydalara əsaslanan metodlar	Süni intellekt və anomaliya analizi
İnformasiya tamlığı	Lokal ehtiyat nüsxələr	Verilənlərin tamlığını təmin edən sistemlər
Strateji hədəf	Sübut toplamaq və günahkarı tapmaq	Hücumu neytrallaşdırmaq və suverenliyi qorumaq

Sİ texnologiyaları redaktor davranışlarının zaman daxilindəki ardıcıllığını izləməyə imkan verir. Ənənəvi metodlar

tək bir redaktəni analiz etdiyi halda, Sİ əsaslı ekspertiza modeli uzunmüddətli "redaktə zəncirini" araşdıraraq, təbii istifadəçi davranışı ilə süni şəkildə idarə olunan (koordinasiyalı) redaktə dalğaları arasındakı anomaliyaları aşkar edir. Bu, informasiya müharibəsinin gizli əlamətlərini – hazırlıq, sızma və kütləvi manipulyasiya mərhələlərini dəqiq şəkildə identifikasiya etməyə şərait yaradır. Təklif olunan proaktiv yanaşmanın ənənəvi metodlarla müqayisəli analizi aşağıdakı cədvəldə əks olunmuşdur:

NƏTİCƏ

Süni intellekt modellərinə söykənən rəqəmsal ekspertiza mexanizmləri, viki-mühitdəki zərərli fəaliyyətlərin arxasında duran gizli şəbəkələri ifşa etməklə yanaşı, məlumatın mənşəyini elmi və hüquqi baxımdan isbat edən proaktiv müdafiə alətinə çevrilmişdir. Mərkəzləşdirilməmiş paylanmış reyestr texnologiyaları (blokçeyn) və semantik süzgəclərin modelə inteqrasiyası, dövlət əhəmiyyətli ensiklopedik resursların 'həqiqət mənbəyi' statusunu alqoritmik səviyyədə qorumağa imkan verir. Bu yanaşma, rəqəmsal suverenliyin təminini sadəcə kiber-hücumlara cavab reaksiyası deyil, həm də milli maraqlara xidmət edən informasiya ekosisteminin bütövlüyünün sistemli müdafiəsi kimi xarakterizə edir. Təklif olunan modelin dövlət idarəçiliyi və milli təhlükəsizlik sistemlərinə inteqrasiyası, ölkənin qlobal informasiya məkanında kiber-dayanıqlılığını artırmaqla yanaşı, strateji qərarların qəbulunda alqoritmik dürüstlük və insan ekspertizasının vəhdətini təmin edən fundamental yol xəritəsi funksiyasını daşıyır.

Deyilənləri nəzərə alaraq tədqiqat nəticələrini belə strukturlaşdırmaq olar:

- Metodoloji yenilik. Süni intellekt əsaslı zaman seriyası və anomaliya analizi vasitəsilə informasiya hücumlarının hələ hazırlıq mərhələsində lokallaşdırılması mexanizmi əsaslandırılmışdır.
- Texnoloji uyğunluq. Dəyişməz zəncirvari kriptoqrafik qeydiyyat üsullarının tamlıq yoxlaması üçün tətbiqi və semantik süzgəclərin vəhdəti, milli əhəmiyyətli resursların dürüstlüyünü qoruyan fundamental müdafiə mexanizmi funksiyasını daşıyır.
- Rəqəmsal ekspert qərarı alqoritmik qərəzliliyi aradan qaldıraraq əldə olunan rəqəmsal sübutların hüquqi-strateji legitimliyini təmin edir.

ƏDƏBİYYAT

[1] I. K. Kwentoa, "Cybersecurity in Digital Sovereignty: Protecting National Digital Ecosystems against Foreign Cyber Infiltration in the Age of Decentralized Technology," Journal of Next-Generation Research 5.0, 2025.

[2] M. Ye, Hybrid War: Survive and Win, in Ukrainian. Kyiv, Ukraine: Vivat Publishing, 2015.

[3] G. Lilienthal and N. Ahmad, "Cyber-attack as inevitable kinetic war," Computer Law & Security Review, vol. 31, no. 3, pp. 390–400, 2015, doi: 10.1016/j.clsr.2015.03.002.

[4] U. Pagallo, "Cyber force and the role of sovereign states in informational warfare," Philosophy & Technology, vol. 28, no. 3, pp. 407–425, 2015, doi: 10.1007/s13347-014-0177-4.

[5] J. Straub, "Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios," Technology in Society, p. 101177, 2019.

[6] L. Kurek, C. Budak, and E. Gilbert, "Wikipedia in wartime: Experiences of Wikipedians maintaining articles about the Russia-Ukraine war," Proceedings of the ACM on Human-Computer Interaction, vol. 9, no. 2, pp. 1–27, 2025.

[7] A. Shoker, "Digital sovereignty strategies for every nation," Applied Cybersecurity & Internet Governance, vol. 1, no. 1, pp. 1–17, 2022, doi: 10.5604/01.3001.0016.0943.

[8] Y. Shen, "Cyber sovereignty and the governance of global cyberspace," Chinese Political Science Review, vol. 1, no. 1, pp. 81–93, 2016.

[9] R. R. Garifullin, "Wikipedia as one of the tools of information war and influence on the educational system," Revista San Gregorio, no. 20, pp. 56–63, 2017.

[10] J. A. Gannon and K. Chávez, "A Wiki-based dataset of military operations with novel strategic technologies (MONSTr)," International Interactions, vol. 49, no. 4, pp. 639–668, 2023.

[11] C. Miller, M. Smith, O. Marsh, K. Balint, C. Inskip, and F. Visser, Information Warfare and Wikipedia. Institute for Strategic Dialogue (CASM Technology), 2022, p. 25.

[12] R. Pershina, B. Soppe, and T. M. Thune, "Bridging analog and digital expertise: Cross-domain collaboration and boundary-spanning tools in the creation of digital innovation," Research Policy, vol. 48, no. 9, p. 103819, 2019, doi: 10.1016/j.respol.2019.103819.

Detecting Manifestations of Information Warfare in the Wikipedia Environment and Digital Forensics

Irada Alakbarova
Institute of Information Technology, Baku, Azerbaijan
airada.09@gmail.com

Abstract- Wikipedia, the world's largest collective knowledge resource, has become an active training ground for information operations and hybrid warfare in recent years. As part of the research, a proactive digital forensics model based on artificial intelligence models has been proposed. The article provides a scientific and theoretical justification for the mechanisms of collecting digital evidence, protecting information integrity, and building a proactive defense system based on user behavior analysis. The proposed new approach may be important for ensuring information security in digital ecosystems and protecting the digital sovereignty of the government.

Keywords- Wikipedia; information warfare; digital forensics; artificial intelligence.