İnsan Sağlamlığına Yönəlmiş Kibertəhlükələr və Onların Rəqəmsal Ekspertizası

Kəmalə Qurbanova[1], Xəyalə Əbdülhüseynova[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*kemalewamil@gmail.com*, [2]*abdulxayala@gmail.com*

***Xülasə*— İnsan sağlamlığına yönəlmiş kibertəhlükələr rəqəmsal mühitdə fərdin biopsixoloji rifahına təsir edən kompleks risklərdir. Tədqiqat işində sosial və psixoloji nəticələr insan faktoru kontekstində təhlil edilmiş, kiberzorakılıq və rəqəmsal asılılıq arasındakı əlaqə araşdırılmışdır. Kibertəhlükələrin aşkarlanması məqsədilə BERT və RoBERTa kimi Transformer arxitekturaları, habelə RNN, LSTM və BiLSTM neyron şəbəkə modelləri əsasında mətni məlumatların intellektual analizi təhlil edilmişdir. Beynəlxalq təcrübədə risklərin yayılma intensivliyi və müdafiə yanaşmaları müqayisə edilmişdir.**

Açar sözlər*— *kibertəhlükə; biopsixoloji rifah; hibrid dərin təlim modelləri; BERT arxitekturası; rəqəmsal ekspertiza.

I. Giriş

Süni intellekt texnologiyaları müasir dövrdə məlumatların analizi və qərar qəbuletmə proseslərinin optimallaşdırılması vasitəsilə cəmiyyətin sosial-iqtisadi inkişafına mühüm töhfə verir. Bununla yanaşı, rəqəmsal transformasiya prosesləri yalnız həyat keyfiyyətini yüksəltməklə məhdudlaşmır, eyni zamanda insan sağlamlığına yönəlmiş yeni tip kibertəhlükələrin formalaşmasına səbəb olur. Kibertəhlükə fərdin həm fiziki, həm də psixoloji rifahına təsir edən kompleks risklər sistemi kimi çıxış edir.

Son illər internet üzərindən edilən psixoloji manipulyasiya və kiberzorakılıq halları ciddi təhlükəyə çevrilib. Nəzarətsiz istifadə fərdləri manipulyasiya edərək onları intihar həddinə qədər çatdıra bilir [1]. Bu kimi proseslər artıq yalnız sosial problem deyil, həm də insan təhlükəsizliyinin və milli təhlükəsizlik paradiqmasının mühüm komponenti kimi qiymətləndirilir. Xüsusilə rəqəmsal mühitdə davranışların idarə olunması və təsirləndirilməsi imkanlarının artması bu sahədə risklərin daha da dərinləşməsinə səbəb olur.

Rəqəmsal mühitdə insan sağlamlığına yönəlmiş kibertəhlükələr coğrafi sərhəd tanımır və internetin əlçatanlığının artması ilə daha geniş yayılmaqdadır. Bu baxımdan, problemin kompleks şəkildə araşdırılması kiber-kriminalistika, psixologiya, sosiologiya və hüquq elmlərinin inteqrasiyasını tələb edir. Müasir yanaşmalar çərçivəsində kibertəhlükələrin aşkarlanması və qarşısının alınması üçün texnoloji əsaslı metodların tətbiqi xüsusi əhəmiyyət kəsb edir.

Rəqəmsal mühitdə psixoloji təsirlər və kibertəhlükələrin yaratdığı risklərin artması məsələsi bir sıra beynəlxalq hüquqi və tibbi sənədlərdə öz təsdiqini tapmışdır: Ümumdünya Səhiyyə Təşkilatının "Beynəlxalq Xəstəliklərin Təsnifatı" (2019) [2], "Kiber-cinayətkarlıq haqqında" Budapeşt Konvensiyası (2001) və onun İkinci Əlavə Protokolu (2021) [3], UNESCO-nun Süni İntellekt Etikası üzrə Tövsiyələri (2021) [4] və s. Bu sənədlərin qəbul edilməsində əsas məqsəd rəqəmsal mühitdə yaranan psixoloji asılılıqların, risklərin və onlayn manipulyasiyaların qarşısının alınması, həmçinin fərdlərin, xüsusilə də uşaqların və yeniyetmələrin biopsixoloji rifahının qorunmasıdır.

Beynəlxalq normativ çərçivələr göstərir ki, virtual mühitin insan psixikasına təsiri artıq qlobal səviyyədə ciddi problem kimi qəbul edilir və bu sahədə hüquqi tənzimləmələrin gücləndirilməsi zəruri hesab olunur. Eyni zamanda, müasir dövrdə keçirilən beynəlxalq forumlar və irəli sürülən təşəbbüslər, xüsusilə süni intellekt və alqoritmik təsirlərlə bağlı müzakirələr, problemin aktuallığını daha da artırır və rəqəmsal təhlükəsizliyin təmin edilməsini qlobal prioritet kimi ön plana çıxarır.

Bu tədqiqatın məqsədi insana zərər vuran kibertəhlükələrin sistemli təsnifatını aparmaq, eləcə də onların rəqəmsal kriminalistika metodları vasitəsilə aşkarlanması və etibarlı sübut bazasının formalaşdırılması yollarını müəyyən etməkdir. Tədqiqatın obyekti rəqəmsal mühitdə fərdin psixoloji sağlamlığına yönəlmiş destruktiv fəaliyyətlər və onların yaratdığı risklərdir. Tədqiqatın predmeti isə həmin risklərin identifikasiyasıdır.

Tədqiqat işində kibertəhlükənin mərhələli təsir mexanizmləri müəyyən edilmiş və onların aşkarlanmasında hibrid dərin təlim modellərinin (BERT, BiLSTM) tətbiqinin yüksək effektivliyi əsaslandırılmışdır. İşin yekununda rəqəmsal sübutların beynəlxalq standartlara uyğun toplanması və ekspertizası üçün multidissiplinar müdafiə istiqamətində təkliflər verilmişdir.

II. Kibertəhlükələrin Sosial və Psixoloji Nəticələri: İnsan Faktoru Kontekstində Analiz

Müasir rəqəmsal transformasiya dövründə kibertəhlükə anlayışı fundamental təkamül mərhələsini keçməkdədir. Əvvəllər kibertəhlükəsizlik dedikdə yalnız texnoloji infrastrukturun, məlumat bazalarının və şəbəkə avadanlıqlarının kənar müdaxilələrdən qorunması nəzərdə tutulurdusa, hazırda diqqət mərkəzi fərdin biopsixoloji təhlükəsizliyinə yönəlmişdir. Bu keçid, kiber-məkanın artıq

DOI: 10.25045/forensic.gov.2026.85

sadəcə məlumat mübadiləsi platforması deyil, insanın emosional və psixi vəziyyətinə təsir göstərən ekosistemə çevrilməsi ilə şərtlənir. Kibertəhdid istifadəçinin biopsixoloji təhlükəsizlik parametrlərinə: fiziki sağlamlığına və psixologiyasına təsir göstərən kompleks risk faktorudur [5].

Psixoloji manipulyasiya texnikaları və məlumat axınını məhdudlaşdıran selektiv alqoritmik filtrlər insanın obyektiv təfəkkür sistemini pozur və onda xroniki emosional gərginlik formalaşdırır. Bu növ kibertəhdidlər texniki boşluqlardan deyil, insanın koqnitiv zəifliklərindən istifadə edir. Fərddə daimi təşviş, depressiya və sosial izolyasiya hissi yaradaraq, onu psixoloji cəhətdən müdafiəsiz vəziyyətə gətirir. Kibertəhdidlərin təsir spektri rəqəmsal asılılıqdan başlayaraq, ağır psixi pozuntular və hətta fərdin özünəqəsd həddinə çatdırılmasına qədər olan geniş spektri əhatə edir. Kibertəhdidlərin insan biopsixoloji sisteminə təsiri mərhələli xarakter daşıyır və müxtəlif klinik nəticələrlə özünü göstərir [6, 7, 8, 9]:

- *Davranış pozuntuları və rəqəmsal asılılıq:* İnternet, sosial media və oyun platformalarına aludəçilik fərdin gündəlik həyat ritmini və yuxu rejimini sarsıdır. Orqanizm yuxu zamanı bioloji bərpa prosesini həyata keçirir. Buna görə də xroniki yuxusuzluq beyin funksiyalarına mənfi təsir göstərərək zehni fəaliyyəti zəiflədir, intellektual işin keyfiyyətini aşağı salır və peşəkar karyerada uğursuzluq riskini artırır. Davamlı rəqəmsal asılılıq diqqət dağınıqlığı və emosional gərginlik yaradaraq klinik psixoloji travmaların təməlini qoyur;
- *Emosional travmalar və sosial izolyasiya:* Onlayn mühitdəki virtual sərbəstlik və sərhədsiz fəaliyyət imkanları fərdi real həyatdan təcrid edərək sosial izolyasiyaya sövq edir. Rəqəmsal kiber-zorakılıq şəxsiyyətin bütövlüyünə zərbə vurur və fərdin özünəinamını sarsıdır. Davamlı onlayn təzyiq və manipulyasiyalar xroniki stressə, emosional tükənməyə və posttravmatik stress pozuntusuna yol açaraq fərdin sosial mühitə inklüziyasını kəskin zəiflədir;
- *Manipulyasiya mexanizmləri və koqnitiv təhriflər:* Alqoritmik filtrləmə prosesləri fərddə yanlış inancların formalaşmasına, reallıq qavrayışının təhrif olunmasına və sosial radikallaşmaya səbəb olur. Psixoloji manipulyasiya texnikaları fərdin iradəsini zəiflədərək, onun davranışlarının kənar subyektlər tərəfindən idarə olunmasına şərait yaradır. Bu proses fərddə dərin psixoloji zədələnmələr yaradaraq onu uzunmüddətli psixi patologiyalarla qarşı-qarşıya qoyur;
- *Kritik və həyati təhlükələr:* Kiber-risklərinin ən aqressiv mərhələsi olan kiber-təqib və psixoloji terror müdaxiləsi fərdin daxili psixoloji müdafiə mexanizmlərini iflic edir. Bu növ hədəfyönlü hücumlar fərdin emosional dayanıqlığını sıradan çıxarır, onda dərin ekzistensial böhran və çıxılmazlıq hissi yaradır. Nəticədə, sistematik onlayn təzyiq və intihara təşviq edən rəqəmsal mühit fərddə özünəqəsd meyillərinin yaranmasına və şəxsiyyətin tam destruksiyasına yol açan kritik həyati risklər doğurur.

Kibertəhdidlərin bu destruktiv təsirləri beynəlxalq səviyyədə hüquqi və tibbi tənzimləmə mexanizmlərinin yenilənməsini zəruri etmişdir. Ümumdünya Səhiyyə Təşkilatının (ÜST) XBT-11 (ICD-11) təsnifatında rəqəmsal oyun asılılığını rəsmi olaraq davranış pozuntusu kimi tanıması, problemin artıq klinik müdaxilə tələb edən tibbi-psixoloji məsələ olduğunu təsdiqləyir [2]. Eyni zamanda, Budapeşt Konvensiyasının İkinci Əlavə Protokolu, xüsusilə kiber-zorakılıq və onlayn mühitdə törədilən şəxsiyyət əleyhinə cinayətlərin araşdırılmasında rəqəmsal sübutların transsərhəd əldə edilməsi mexanizmlərini təkmilləşdirir [3].

Qlobal miqyasda BMT, UNESCO və ÜST tərəfindən irəli sürülən standartlar isə məsələyə rəqəmsal rifah (digital wellbeing) və kiber-etika müstəvisindən yanaşır. UNESCO-nun süni intellekt etikasına dair tövsiyələri və ÜST-ün rəqəmsal sağlamlıq üzrə 2026-cı il hədəfləri, texnologiyanın insan mənfəətinə xidmət etməsini və alqoritmik manipulyasiyaların fərdin psixi bütövlüyünə zərər verməməsini tələb edir [4]. Beləliklə, beynəlxalq hüquqi çərçivə texnoloji inkişafla insan sağlamlığı arasında balansın qorunmasını hədəfləyən vahid bir müdafiə sistemi formalaşdırır. Bu kontekstdə kibertəhdidlərin vaxtında aşkarlanması və destruktiv fəaliyyətlərin hüquqi müstəvidə sübuta yetirilməsi üçün rəqəmsal ekspertiza metodlarının tətbiqi zərurətə çevrilmişdir.

III. İNSAN SAĞLAMLIĞININ KİBERTƏHLÜKƏDƏN MÜHAFİZƏSİ: MULTİDİSSİPLİNAR TƏDBİRLƏR

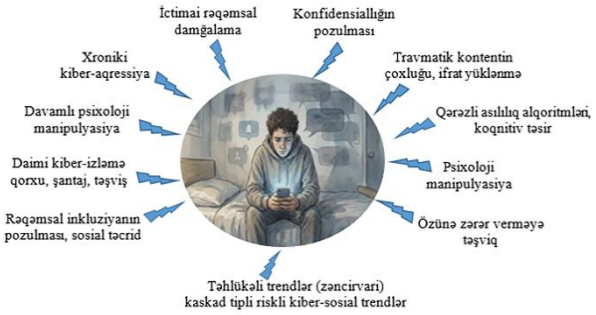
Kibertəhlükələrin rəqəmsallaşma və sosiallaşmanın getdikcə daha çox formalaşdırdığı cəmiyyət kontekstində, zorakılıq və ya təzyiq yeniyetmələrin psixi sağlamlığına getdikcə daha çox zərər vuran mühüm risk faktoruna çevrilmişdir. Son qlobal hesabatlar göstərir ki, yeniyetmələrin təxminən 30%-i onlayn mühitdə qurbana çevrilmişdir. Təzyiqə məruz qalmaq yeniyetmələrdə depressiya, təşviş, özünəzərərvermə davranışları və intihar meyillərinin yaranma riskini əhəmiyyətli dərəcədə artmışdır. Virtual sosial platformalarda reallaşan hücumlar anonimlik, davamlılıq, geniş yayılma imkanları ilə seçilir ki, bu da qurbanların təzyiqdən qaçmasını və ya dərhal dəstək almasını çətinləşdirir [10].

Kibertəhlükələrin yaratdığı dağıdıcı maliyyə itkiləri və reputasiya risklərindən qorunmaq üçün sistemli idarəetmə çərçivələrinin strateji inteqrasiyası həlledici əhəmiyyət kəsb edir. NIST Kibertəhlükəsizlik Çərçivəsi (CSF), ISO/IEC 27001 və ya CIS Kontrolları kimi beynəlxalq standartların mənimsənilməsi təşkilatlara həm normativ-hüquqi uyğunluğu təmin etmək, həm də kibertəhlükələrə qarşı ümumi dayanıqlıq səviyyəsini əhəmiyyətli dərəcədə yüksəltmək imkanı verir. Tədqiqatlar göstərir ki, NIST-in çevik, risk-əsaslı yanaşması ilə ISO 27001-in strukturlaşdırılmış idarəetmə sistemlərinin (ISMS) müqayisəli tətbiqi müdafiə mexanizmlərinin effektivliyini artırır. Bu proses yalnız texnoloji infrastrukturun yenilənməsini deyil, həm də bütün maraqlı tərəflərin iştirakı ilə

korporativ təhlükəsizlik mədəniyyətinin formalaşdırılmasını və dinamik təhdid mənzərəsinə uyğun olaraq nəzarət mexanizmlərinin davamlı təkmilləşdirilməsini tələb edir [11].

Bu yanaşma göstərir ki, rəqəmsal mühitdə kibertəhlükələrin mürəkkəbləşməsi insanın psixoloji və sosial rifahının qorunması cəmiyyətin qarşısında duran məsələdir. Risklərin qiymətləndirilməsi tamamlandıqdan sonra təşkilatlar və rəqəmsal platformalar müəyyən edilmiş bu spesifik təhlükələrə uyğunlaşdırılmış effektiv risk idarəetmə strategiyalarını tətbiq etməlidirlər. Bu strategiyalar yalnız qoruma funksiyası daşımamalı, həm də rəqəmsal sübutların formalaşdırılması və sonradan ekspertiza prosesində istifadəsini təmin etməlidir. Bu baxımdan yanaşma üç qatlı müdafiə tədbirinə əsaslanır [12]:

- *Qabaqlayıcı tədbirlər*: Bu tədbirlər insan sağlamlığına yönəlmiş kibertəhlükələrin (məsələn, psixoloji təzyiq, zərərli kontent, manipulyativ təsirlər) baş verməsinin qarşısını almağa xidmət edir (Şəkil 1). Əsas məqsəd yalnız texniki zəifllikləri deyil, həm də istifadəçi davranışına təsir edən risk faktorlarını erkən mərhələdə aradan qaldırmaqdır. Bu çərçivədə kontent filtrasiyası, istifadəçi identifikasiyası, platforma təhlükəsizlik siyasətləri və davranış əsaslı nəzarət mexanizmləri tətbiq olunur. Eyni zamanda bu tədbirlər istifadəçi fəaliyyətinin qeydiyyatını təmin etməklə gələcəkdə mümkün rəqəmsal ekspertiza üçün ilkin məlumat bazasının formalaşmasına şərait yaradır;



Şəkil 1. İnsan yönümlü kibertəhlükələrin struktur-məntiqi sxemi

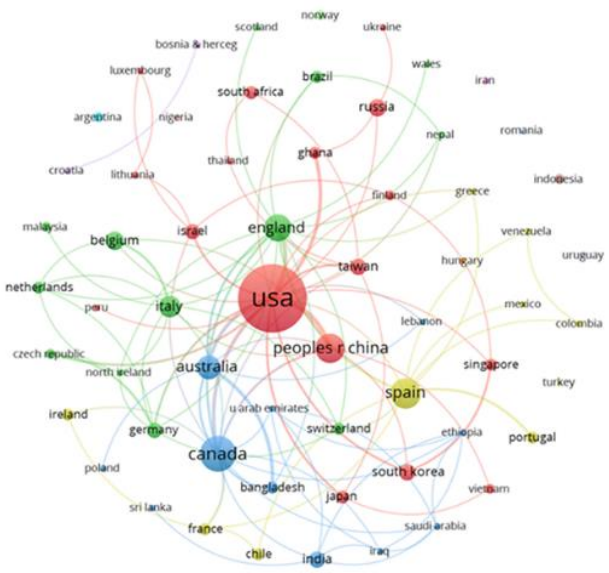
- *Aşkarlayıcı tədbirlər*: Bu tədbirlər qabaqlayıcı müdafiə qatını keçmiş və ya baş verməkdə olan insan yönümlü kibertəhlükələrin aşkarlanmasına yönəlib. Onlar real-vaxt rejimində anomaliyaları, psixoloji təzyiq hallarını və digər zərərli davranış modellərini müəyyən etməyə xidmət edir. Bu mərhələdə sistem loqlarının analizi, istifadəçi fəaliyyətinin monitorinqi, mesajlaşma və sosial media məlumatlarının təhlili kimi üsullar tətbiq olunur. Məhz bu prosesdə toplanan məlumatlar rəqəmsal sübutların əsasını təşkil edir və sonradan rəqəmsal ekspertiza zamanı hadisənin səbəb-nəticə əlaqələrinin müəyyən olunmasında istifadə olunur;
- *Korrektiv (korreksiyaedici) tədbirlər:* Bu tədbirlər təhlükəsizlik insidenti baş verdikdən sonra işə düşür. Məqsəd zərəri minimuma endirmək, sistemin fəaliyyətini bərpa etmək və gələcəkdə bənzər hadisələrin təkrarlanmaması üçün boşluqları aradan qaldırmaqdır. İnsidentə reaksiya planları (IRP), ehtiyat nüsxələrdən bərpa (backup), sistem yamaqlarının (patches) tətbiqi və fəlakətdən sonra bərpa (DRP) kimi tədbirlər müvafiq protokollar vasitəsilə həyata keçirilir;

Qabaqlayıcı və aşkarlayıcı müdafiə qatlarının effektivliyi insan yönümlü təhdidlərin real-vaxt rejimində və yüksək dəqiqliklə aşkarlanması imkanlarından asılıdır. İnsan psixologiyasına yönəlmiş bu mürəkkəb hücumların qarşısının alınması üçün müasir intellektual alqoritmlərin tətbiqi zərurətə çevrilmişdir.

IV. Kibertəhlükə Probleminin Beynəlxalq Elmi-Praktiki Müstəvidə Multidissiplinar Təhlili

Sürətli rəqəmsallaşma fərdlərin sosial mühitini köklü şəkildə dəyişmişdir. Rəqəmsal platformalar artıq müasir insanın gündəlik həyatının və fərdi inkişafının ayrılmaz hissəsidir. Lakin internetə çıxış imkanlarının genişlənməsi və mobil texnologiyaların kütləviləşməsi yeni risklər formalaşdırıb. Bu kontekstdə hər bir yaş qrupunun psixoloji rifahına təhdid yaradan kibertəhlükə qlobal miqyaslı bir problemə çevrilmişdir.

Beynəlxalq tədqiqatlar göstərir ki, rəqəmsal mühitdə zorakı və zərərli davranışlar coğrafi və sosial-iqtisadi sərhədlərdən asılı olmadan yayılır. Bu hallar fərdlərin psixoloji vəziyyətinə mənfi təsir göstərir və cəmiyyətdə aqressiv davranışların artmasına səbəb olur. Rəqəmsal əlaqəliliyin və istifadə intensivliyinin yüksək olduğu mühitlərdə bu tip məzmunların ötürülmə sürəti və əhatə dairəsi artır. Bu isə rəqəmsal mühitdə risklərin idarə olunmasını və nəzarət mexanizmlərinin gücləndirilməsini zəruri edir. Kibertəhlükə halları rəqəmsal aktivliyin yüksək olduğu ölkələrdə, xüsusilə ABŞ-da daha geniş yayılma meyli göstərir (Şək. 2). Bu, yüksək istifadəçi sıxlığı və platforma əlçatanlığı ilə əlaqədar olaraq zərərli məzmunun ötürülmə intensivliyinin artması ilə izah olunur [13].



Şəkil 2. Ölkələr üzrə kiber-zorakılıq və rəqəmsal risklərin yayılma intensivliyi

[14]-cü işdə aparılan tədqiqatın nəticələrinə görə, kibertəhlükəyə məruz qalma intihar cəhdlərinin əsas proqnozlaşdırıcı göstəricilərindən biri kimi müəyyən edilmişdir. Bu, rəqəmsal mühitdə zorakılıqla intihar cəhdləri arasında əlaqənin mövcudluğu ilə əlaqədardır. Tədqiqat göstərir ki, bu əlaqə çoxşaxəli və kompleks xarakter daşıyır, rəqəmsal təzyiq fiziki zorakılığa nisbətən daha yüksək risk yaradır.

İnsan sağlamlığına yönəlmiş kibertəhlükələr müxtəlif formalarda təzahür edir və əsasən fərdin psixoloji vəziyyətinə təsir edən dağıdıcı mexanizmlərlə xarakterizə olunur. Araşdırma sübut edir ki, bu problem qlobal xarakter daşısa da, onun intensivliyi və təsir mexanizmləri ölkələrin sosial-iqtisadi xüsusiyyətlərindən asılı olaraq dəyişir. Müxtəlif beynəlxalq hesabatlara əsasən, yeniyetmələr arasında kibertəhdid göstəriciləri əksər ölkələrdə 12–20% intervalında dəyişir, lakin geniş təriflə ölçüldükdə bu göstərici bəzi ölkələrdə 60%-ə qədər yüksəlir. 2025-ci ildə ABŞ-da Tədqiqat Mərkəzi tərəfindən aparılan statistikaya əsasən gənclər arasında kiberzorakılığa və rəqəmsal təcavüzə məruz qalma nisbəti 58,2% təşkil edir [15].

Bu sahədə aparılan beynəlxalq tədqiqatların nəticələri rəqəmsal asılılıq və kiberzorakılıq riskləri arasında əlaqənin olduğunu təsdiqləyir [15]:

- OECD-nin məlumatına əsasən, inkişaf etmiş ölkələrdə 15 yaşlı yeniyetmələrin 97%-dən çoxu hər gün internetdən istifadə edir;
- Avropa Birliyi Uşaq İştirakı Platformasının 2025-ci il hesabatına görə, yetkinlik yaşına çatmayanların 24%-i onlayn mühitdə təcavüzlə üzləşir;
- ÜST-ün 2024-cü il HBSC tədqiqatının nəticələrinə görə, Avropa regionunda hər altı yeniyetmədən biri kiberzorakılığın qurbanına çevrilir ki, bu da son illərdə problemin miqyasının sürətlə genişləndiyini sübut edir.

[16]- ci tədqiqat işində kibertəhlükələrin aşkarlanması və rəqəmsal ekspertizası istiqamətində qlobal elmi mühitdə yüksək nüfuza malik olan tədqiqatçıların biblioqrafik analizi təqdim olunur. Bu sahədə fundamental biliklərin formalaşmasında və nəzəri paradiqmaların qurulmasında müstəsna xidmətləri olan müəlliflər, həm nəşr etdikləri məqalələrin sayı (məhsuldarlıq), həm də beynəlxalq elmi ictimaiyyət tərəfindən alınan istinadların həcmi əsasında müəyyən edilmişdir. Cədvəl 1-də sahənin ən nüfuzlu simaları, onların akademik mənsubiyyəti və elmmetrik göstəriciləri ətraflı şəkildə əks olunmuşdur..

[17]-ci işdə isə sosial şəbəkələrdə kibertəhlükələrin aşkarlanması və ekspertizası, eləcə də maşın öyrənməsi metodlarının tətbiqi istiqamətində biblioqrafik analiz aparmışlar. Nəticələr göstərmişdir ki, bu sahədə elmi məhsuldarlığa görə qlobal liderlik Hindistana məxsusdur (Şəkil 3). Tədqiqatın coğrafi paylanması kifayət qədər geniş olub, 46 ölkəni və 193 müxtəlif elmi-tədris müəssisəsini əhatə edir ki, bu da problemin qlobal aktuallığını bir daha təsdiq edir.

Kibertəhlükənin coğrafi sərhəd tanımayan qlobal xarakteri və insan həyatına təsiri müasir elmi ictimaiyyətin diqqət mərkəzindədir. Problemin mürəkkəbliyi dünyada genişmiqyaslı elmi tədqiqatlara yol açmışdır. Beynəlxalq müstəvidə bir çox konseptual yanaşmalar irəli sürülmüşdür. Bu yanaşmalar içərisində süni intellekt və dərin təlim modelləri xüsusi əhəmiyyət kəsb edir.

CƏDVƏL I. KİBERTƏHLÜKƏ VƏ RƏQƏMSAL RİSKLƏR ÜZRƏ APARICI TƏDQİQATÇILARIN ELMMETRİK GÖSTƏRİCİLƏRİ

Müəllif	Akademik Müəssisə / Ölkə	Məqalə	İstinad
Robin Kowalski	University of Texas Arlington / USA	**3**	**1178**
Sameer Hinduja	Florida Atlantic University / USA	**4**	**1044**
Justin W. Patchin	University of Wisconsin System / USA	**4**	**1044**
Sheri Bauman	University of Arizona / USA	**4**	**394**
Anat Brunstein Klomek	Reichman University / Israel	**3**	**263**
Hugues Sampasa-Kanyinga	University of Ottawa / Canada	**4**	**174**
Cira Quintana-Orts	University of Sevilla / Spain	**5**	**105**
Lourdes Rey	University of Malaga / Spain	**5**	**105**
Patrick Baiden	University of Texas Arlington / USA	**7**	**99**
Jude Mary Cénat	University of Ottawa / Canada	**3**	**96**
Martine Hébert	University of Quebec Montreal / Canada	**3**	**96**
Ilse De Bourdeaudhuij	Ghent University / Belgium	**3**	**82**
Ann DeSmet	Universite Libre de Bruxelles / Belgium	**4**	**82**
Wen-Jiun Chou	Chang Gung Memorial Hospital / Taiwan	**3**	**75**
Tai-Ling Liu	Kaohsiung Medical University Hospital / Taiwan	**3**	**75**

Şəkil 3. Kibertəhlükələrin aşkarlanması üzrə elmi tədqiqatların qlobal coğrafi məhsuldarlıq xəritəsi

V. KİBERTƏHLÜKƏNİN AŞKARLANMASINA DƏRİN TƏLİM MODELLƏRİNİN TƏTBİQİ (MÖVCUD YANAŞMALAR)

Rəqəmsal transformasiya mühitində sosial şəbəkələr, onlayn oyun platformaları və dağıdıcı ideoloji qrupların geniş yayılması kibertəhlükələrin miqyasını artıraraq fərdi və ictimai təhlükəsizlik üçün ciddi risk amilinə çevrilmişdir.

Fərdlərin psixoloji və fiziki sağlamlığına yönəlmiş bu təhdidlər əsasən insanların inamından sui-istifadə edən rəqəmsal platformalar, saxta məlumat və kiber-təqib mənbəyinə çevrilən sosial şəbəkələr (Twitter, İnstaqram, Teleqram, Feysbuk və s.), eləcə də asılılıq yaradan onlayn oyun mühitləri vasitəsilə formalaşır. Sözügedən risklər insanların intihar

həddinə çatdırılması və psixoloji pozuntuların dərinləşməsi məqsədilə qeyri-rəsmi mənbələr tərəfindən qlobal miqyasda yayılır.

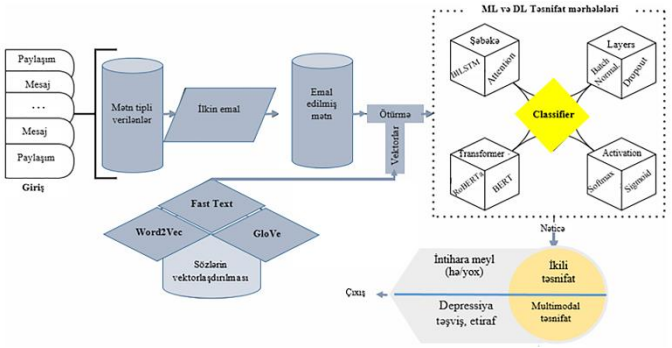
Şəbəkə daxilindəki anonimlik, məlumatların sürətli dövriyyəsi və coğrafi sərhədlərin olmaması kiber-aqressiv davranışların fəsadlarını artıraraq, bu növ insidentlərin müəyyən edilməsi və rəqəmsal ekspertizası prosesini mürəkkəbləşdirir. Süni intellektin mövcud inkişaf mərhələsində maşın təlimi modelləri aşkarlama dəqiqliyi baxımından müəyyən məhdudiyyətlərlə qarşılaşır. Bu kontekstdə, müxtəlif alqoritmlərin birgə tətbiqinə əsaslanan metodologiya, böyük həcmli və çoxşaxəli məlumat axınlarında kiber-zorakılıq hallarının yüksək dəqiqliklə müəyyən edilməsini təmin edən effektiv vasitə hesab olunur [18].

Kiber-zorakılıq hallarının analizi zamanı mətnin yalnız lüğəvi mənası deyil, eyni zamanda onun daşıdığı kontekstual çalar həlledici rol oynayır. Bu mürəkkəbliyin aradan qaldırılmasında BERT (Bidirectional Encoder Representations from Transformers) modeli inqilabi yanaşma təqdim edir. Klassik modellərdən fərqli olaraq, BERT texnologiyası mətni hər iki istiqamətdə (sağdan sola və soldan sağa) eyni vaxtda analiz edərək, sözlərin əhatə olunduğu cümlə daxilindəki dəqiq semantik mənasını müəyyənləşdirir. Bu, xüsusilə sarkazm, gizli hədə-qorxu və mürəkkəb emosional vəziyyətlərin aşkarlanmasında yüksək dəqiqlik nümayiş etdirərək, tədqiqatın texnoloji bazasını gücləndirir [19].

[20] saylı tədqiqatda özünəqəsd meyllərinin təsnifatı üçün təklif olunan hibrid model arxitekturası işlənmişdir. Tədqiqat çərçivəsində mətn tipli məlumatların intellektual analizi və təsnifatı məqsədilə kompleks metodoloji çərçivə işlənib hazırlanmışdır (Şək. 4). Bu arxitektura, xam məlumatın daxil olmasından başlayaraq, müasir dərin öyrənmə alqoritmləri vasitəsilə yüksək dəqiqlikli nəticələrin əldə edilməsinə qədər olan çoxmərhələli bir prosesi əhatə edir. Modelin mərhələli iş mexanizmi aşağıdakı kimidir:

- *Verilənlərin ilkin emalı:* Giriş blokuna daxil olan müxtəlif xüsusiyyətli verilənlər ilkin mərhələdə strukturlaşdırılmış mətnə çevrilir;
- *Kodlaşdırma:* Word2Vec, fastText və GloVe modelləri vasitəsilə sözlər riyazi vektorlara çevrilərək təsnifat üçün növbəti bloka ötürülür;
- *Dərin təlim metodları*: Modelin nüvəsini təşkil edən bu hissədə BiLSTM və Attention mexanizmləri mətnin kontekstual asılılıqlarını, BERT və RoBERTa transformerləri isə semantik mənasını analiz edir;
- *Tənzimləmə:* Modelin həddindən artıq təliminin qarşısını almaq üçün arxitekturaya Dropout və Batch Normalization qatlamları inteqrasiya edilmişdir;
- *Təsnifatlandırma:* Verilənlərin xüsusiyyətindən asılı olaraq, ikili təsnifat üçün Sigmoid, çoxsinifli təsnifat üçün isə Softmax aktivasiya funksiyaları tətbiq olunur;
- *Nəticə və ya çıxış:* Kibertəhlükə riski aşkarlanır.

Təqdim olunan yanaşmalar göstərir ki, kibertəhlükələrin aşkarlanması sahəsində BERT əsaslı modellər və hibrid ansambl metodologiyaları yüksək dəqiqlik və ümumiləşdirmə qabiliyyəti ilə seçilir. Kontekstual semantikanın dərin təhlili və müxtəlif modellərin inteqrasiyası daha etibarlı və dayanıqlı nəticələrin əldə olunmasına şərait yaradır.



Şəkil 4. Kibertəhlükələrin aşkarlanması üçün süni intellekt əsaslı hibrid dərin təlim modelinin ümumi arxitekturası

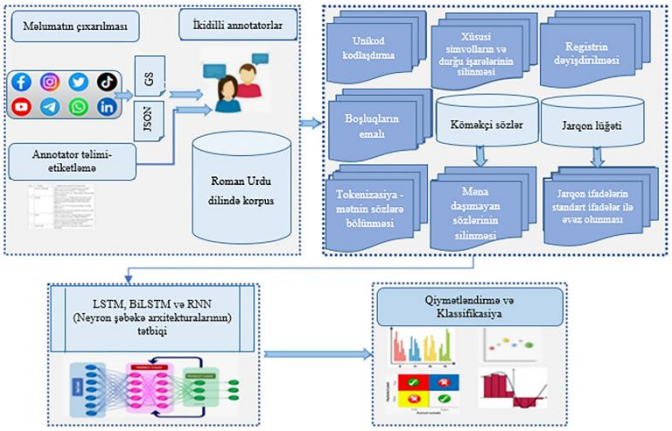
BERT və digər transformer əsaslı modellər mətnin kontekstual semantikasını yüksək dəqiqliklə analiz etmək imkanları ilə seçilsə də, kibertəhlükənin aşkarlanması sahəsində daha əvvəlki mərhələlərdə ənənəvi dərin təlim modellərinə əsaslanan yanaşmalar da geniş tətbiq edilmişdir. Bu yanaşmalar, xüsusilə mətnin ardıcıllıq xüsusiyyətlərini öyrənmək baxımından effektiv olan RNN, LSTM və BiLSTM kimi arxitekturalara əsaslanaraq, müxtəlif dillərdə və verilənlər bazalarında praktik nəticələr təqdim etmişdir.

[21] saylı tədqiqatda kibertəhlükənin aşkarlanması prosesi kompleks bir strukturda təqdim edilmişdir (Şəkil 5). Təklif olunan sxem məlumatların ilkin toplanmasından başlayaraq yekun analitik qiymətləndirməyə qədər davam edən ardıcıl dörd əsas metodoloji mərhələni əks etdirir:

- *Məlumatların ekstraksiyası və annotasiyası:* Sosial platformalardan xam məlumatların çıxarılması və etiketlənməsi: Sosial şəbəkədən məlumat çıxarılır, Google Sheets (GS) və JSON formatında saxlanılır, ikidilli annotatorlar məlumatı etiketləyir, Roman Urdu dilində korpus yaradılır;
- *Genişləndirilmiş ilkin emal:* Mətnin təmizlənməsi (hərflərin registrinin vahid formaya salınması) və Roman Urdu dili üçün spesifik məna daşımayan (stop) sözlərin çıxarılması, həmçinin tokenizasiya (mətni analiz üçün hissələrə ayırır) kimi linqvistik normallaşdırma (jarqon ifadələrin standart ifadələr ilə əvəz olunması) mərhələlərinin tətbiqi: Unicode/encoding düzəlişi, xüsusi simvolların silinməsi, kiçik/böyük hərf çevrilməsi, məna kəsb etməyən sözlərin çıxarılması, tokenizasiya və linqvistik normallaşdırma;
- *Modelin arxitekturası və icrası:* Mətnin rəqəmsal vektorlara çevrilməsi və ardıcıl zaman asılılıqlarını idarə edən RNN, LSTM və BiLSTM neyron şəbəkə modellərinin tətbiqi;
- *Qiymətləndirmə və klassifikasiya:* Bu mərhələdə qurulmuş modellərin nə dərəcədə düzgün işlədiyi real

məlumatlar üzərində yoxlanılır. Alınmış nəticələr itki və dəqiqlik funksiyaları ilə analiz edilir.

Burada itki funksiyası modelin təlimi prosesində səhvlərinin necə azaldığını və düzgün proqnozlarının necə artdığını göstərir, əgər itki azalır və dəqiqlik artırsa, model düzgün öyrənir, əks halda modeldə problem ola bilər. Dəqiqlik matrisi isə, modelin proqnozlarını daha detallı qiymətləndirməyə imkan verir və göstərir ki, model hansı hallarda düzgün, hansı hallarda səhv qərar verir. Bu mərhələ modelin sadəcə ümumi nəticəsini deyil, həm də onun zəif və güclü tərəflərini müəyyən etməyə imkan verir.



Şəkil 5. Kibertəhlükə risklərinin identifikasiyası üçün təklif olunan BERT-əsaslı hibrid dərin təlim arxitekturası

Sistem tərəfindən hər bir məlumat vahidi təhlükəli və ya təhlükəsiz olaraq qiymətləndirilir və nəticədə mətnlərin avtomatik klassifikasiyası həyata keçirilərək onların uyğun olaraq hansı sinfə aid olduğu müəyyən edilir.

Təqdim olunan yanaşmalar göstərir ki, BERT arxitekturası ilə yanaşı RNN, LSTM və BiLSTM modelləri kibertəhlükələrin aşkarlanmasında yüksək effektivliyə malikdir. BERT və onun hibrid variantları mətndəki gizli emosional indikatorları və mürəkkəb semantik əlaqələri yüksək dəqiqliklə identifikasiya edir. Bununla yanaşı, rekurrent əsaslı ardıcıl strukturlu modellər müxtəlif dil korpuslarında və çoxmərhələli ilkin emal proseslərində texniki çevikliyini qoruyur.

Yekun olaraq, kibertəhlükələrin və özünəqəsd meyllərinin müəyyən edilməsində bu arxitekturaların sintezi həlledici rol oynayır. Bu yanaşma linqvistik analizin dəqiqliyini artırmaqla bərabər, kiber-təhlükəsizlik sistemlərinin rəqəmsal ekspertiza imkanlarını strateji səviyyədə gücləndirir

VI. Rəqəmsal Ekspertiza Bazasının Formalaşdırılması

Müasir dövrdə insan sağlamlığına yönəlmiş kibertəhlükələrin artması onların yalnız aşkarlanmasını deyil, həm də hüquqi baxımdan sübut olunmasını zəruri edir. Bu baxımdan rəqəmsal ekspertiza kibertəhlükələrin araşdırılmasında əsas metodoloji istiqamətlərdən biridir. Rəqəmsal ekspertiza prosesinin əsas məqsədi rəqəmsal mühitdə baş vermiş hadisələrin obyektiv şəkildə toplanması və onların hüquqi qüvvəyə malik formada təqdim edilməsidir [22].

İnsan sağlamlığına təsir edən kibertəhlükələr kontekstində rəqəmsal sübutlar əsasən sosial media platformaları, mesajlaşma tətbiqləri, e-poçt yazışmaları və istifadəçi fəaliyyətini əks etdirən loq faylları vasitəsilə əldə olunur. Bu sübutlara mətn mesajları, şəkillər, video materiallar, IP ünvanlar, tarix və istifadəçi davranışına dair digər metadata daxildir. Xüsusilə kibertəhlükə, kiber-təqib və intihara təşviq hallarında bu məlumatlar hadisənin səbəb-nəticə əlaqələrinin müəyyən edilməsində mühüm rol oynayır.

Rəqəmsal ekspertiza prosesində məlumatların tamlığının qorunması və təhrif olunmasının qarşısının alınması əsas prinsiplərdən biridir. Bu prinsipi təmin etmək məqsədi ilə ISO/IEC 15408 (Common Criteria) standartı çərçivəsində rəqəmsal ekspertiza metodologiyası və Avropa İttifaqının məlumat qoruması haqqında (General Data Protection Regulation) normaları tətbiq edilir. ISO/IEC 15408 standartı çərçivəsində rəqəmsal sistemlərin dizaynı sübutların etibarlılığını və hüquqi keçərliliyini təmin edən əsas mexanizmlərdən biri hesab olunur. Bu çərçivədə aşağıdakı funksiyalar tətbiq edilir [23]:

- *Giriş nəzarəti*: Qeyri-qanuni müdaxilələrin və icazəsiz girişlərin bloklanması;
- *İstifadəçi atributasiyası*: Hər bir əməliyyatın konkret istifadəçi ilə eyniləşdirilməsi;
- *Zamanın qeyd edilməsi*: Hadisələrin dəqiq vaxt ardıcıllığı ilə qeydiyyata alınması;
- *Məlumatların saxlanılması*: Rəqəmsal sübutların müəyyən edilmiş müddət ərzində mühafizəsi;
- *Məlumat tamlığı*: İnformasiyanın dəyişdirilmədən və təhrif edilmədən saxlanılması;
- *Hüquqi uyğunluq*: Normativ aktlara və tənzimləyici tələblərə tam riayət olunması.

Süni intellekt və maşın öyrənməsi metodlarının inteqrasiyası ekspertiza prosesinin effektivliyini artıraraq vaxt itkisini önləyir və insan amilindən qaynaqlanan xətaları minimuma endirir və effektivliyini əhəmiyyətli dərəcədə artırır.

Beləliklə, rəqəmsal ekspertiza insan sağlamlığına yönəlmiş kibertəhlükələrin araşdırılmasında texniki vasitələrlə yanaşı, eyni zamanda hüquqi və elmi əsaslandırma mexanizmi də tələb olunur. Bu sahədə müasir texnologiyaların tətbiqi risklərin daha dəqiq identifikasiyasına və onların qarşısının alınmasına imkan verir.

Nəticə

Tədqiqat nəticəsində müəyyən edilmişdir ki, psixoloji manipulyasiya, rəqəmsal asılılıq və kiber-zorakılıq kimi amillər fərdin biopsixoloji sistemində mərhələli və dərin destruktiv təsirlər formalaşdırır. Bu təsirlər ilkin mərhələdə emosional gərginlik və davranış pozuntuları ilə müşahidə olunsa da, sonrakı mərhələlərdə ağır psixi pozuntulara və həyati risklərə qədər inkişaf edə bilir. Bu dinamika, kibertəhlükələrin erkən aşkarlanması və preventiv müdaxilə mexanizmlərinin formalaşdırılmasının zəruriliyini əsaslandırır.

Eyni zamanda, süni intellekt və dərin təlim modellərinin

tətbiqi kibertəhlükələrin aşkarlanması sahəsində keyfiyyətcə yeni mərhələ formalaşdırır. Xüsusilə kontekstual semantikanı analiz edən hibrid yanaşmalar zərərli kontentin, psixoloji təzyiq elementlərinin və gizli risk indikatorlarının yüksək dəqiqliklə müəyyən edilməsinə imkan verir. Bu texnoloji imkanlar həm yalnız monitorinq funksiyası daşımır, həm də rəqəmsal ekspertiza üçün etibarlı sübut bazasının formalaşdırılmasına xidmət edir.

Rəqəmsal ekspertiza mexanizmlərinin inkişafı kibertəhlükələrin hüquqi müstəvidə qiymətləndirilməsi və sübuta yetirilməsi baxımından xüsusi əhəmiyyət kəsb edir. Sübutların toplanması, saxlanılması və analizinə dair beynəlxalq standartların tətbiqi bu sahədə obyektivliyin təmin olunmasına şərait yaradır, hüquqi mexanizmlərin effektivliyini artırır və insan hüquqlarının qorunmasına xidmət edir.

Beləliklə, insan sağlamlığına yönəlmiş kibertəhlükələrin qarşısının alınması üçün texnoloji, psixoloji və hüquqi komponentlərin inteqrasiyasına əsaslanan multidissiplinar yanaşma çərçivəsində aşağıdakı tədbirlərin həyata keçirilməsi məqsədəuyğun hesab olunur:

- Rəqəmsal mühitdə psixoloji risklərin erkən aşkarlanması üçün intellektual monitorinq sistemlərinin tətbiqi;
- Kiber-zorakılıq və özünəqəsd meyllərinin identifikasiyası üçün hibrid dərin təlim modellərinin inkişaf etdirilməsi;
- Rəqəmsal sübutların toplanması və ekspertizası üzrə vahid metodoloji çərçivənin formalaşdırılması;
- Sosial platformalarda zərərli və manipulyativ kontentin qarşısının alınmasına yönəlmiş nəzarət mexanizmlərinin gücləndirilməsi;
- Rəqəmsal təhlükəsizlik və psixoloji sağlamlıq üzrə maarifləndirmə tədbirlərinin genişləndirilməsi;
- Ölkədaxilində milli və beynəlxalq səviyyədə hüquqi tənzimləmə mexanizmlərinin təkmilləşdirilməsi.

Nəticə etibarilə, rəqəmsal mühitdə insanın biopsixoloji rifahının qorunması davamlı elmi tədqiqatlar, institusional əməkdaşlıq və sosial məsuliyyət prinsiplərinə əsaslanan kompleks yanaşma ilə mümkündür.

ƏDƏBİYYAT

[1] С. А. Сашенков, "Криминогенное влияние социальных сетей на несовершеннолетних", Вестник Воронежского института МВД. России, 2015, №. 3, с.215-219.

[2] H. M. Pontes et al., "Measurement and conceptualization of Gaming Disorder according to the World Health Organization framework: The development of the Gaming Disorder Test", International journal of mental health and addiction, 2021, vol. 19 (2), pp.508-528.

[3] A. Campina, C. Rodrigues, "Cybercrime and the council of europe Budapest convention: prevention, criminalization, and international cooperation", The Book of Full Papers-7th International Zeugma Conference on Scientific Researches. IKSAD, 2022, vol. 1 (1), pp.112-123.

[4] M. K. K.Alsbou, Y. J. J. Alawneh, "Developing Policies for Ethical Use of AI in Education: A Global Perspective", 3rd International Conference on IoT, Communication and Automation Technology (ICICAT). IEEE, 2025, pp.1-7.

[5] T. Sobb, N. Moustafa and B.Turnbull, "Responsible resilience in cyber–physical–social systems: A new paradigm for emergent cyber risk modeling" Future Internet, 2025, vol. 17 (7), pp.282(1-24).

[6] B. Kumar, S. K. Mathew, "The dark side of social networking sites: A review of cybercrime research" Pacific Asia Journal of the Association for Information Systems, 2024, vol. 16 (3), pp.1-31.

[7] M. Saleem, R. Kumar, C. Chawla, and M. Singh, "Understanding the Human Factors in the Psychology of Cyber Threats", Human Impact on Security and Privacy: Network and Human Security, Social Media, and Devices, IGI Global Scientific Publishing, 2025, pp.39-52.

[8] M. O. Ijiga, H. S. Olarinoye, F. A. B. Yeboah, and J. N. Okolo, "Integrating behavioral science and cyber threat intelligence (CTI) to counter advanced persistent threats (APTs) and reduce human-enabled security breaches", International Journal of Scientific Research and Modern Technology, 2025, vol. 4 (3), pp.1-15.

[9] S. V. Silbert Jose, "Social Networks a Machinery to Commit Suicide: Cyber Bullying and Virtual Games Leading to Cruelty-A Case on Indian Youth", Informatics and Digitalization for Sustainable Development and Well-Being, Cham: Springer Nature Switzerland, 2025, pp.23-30.

[10] A. Hu, L.Bai, Y. Sun, and C. Lin, "Exploring the Effects of Traditional and Cyberbullying Victimization on Chinese Adolescents' Mental Health: Emotion Regulation as a Mediator and Family Support as a Moderator", Sage Open, 2025, vol. 15 (4), Pp. 21582440251394096.

[11] M. Alshar'e, "Cyber security framework selection: Comparision of NIST and ISO27001", Applied computing Journal, 2023, pp. 245-255.

[12] F. Dine "Cyber threat analysis and the development of proactive security strategies for risk mitigation", 2024, pp 1-14. https://www.researchgate.net/publication/384365805_Cyber_Threat_Analysis_and_the_Development_of_Proactive_Security_Strategies_for_Risk_Mitigation

[13] G. Amidu, "The Impact of Cyberbullying on Help-Seeking Among Depressed Young adults in the United States", International Journal of Scientific and Research Publications, 2025, vol 15 (8), pp. 291-303. https://dx.doi.org/10.29322/IJSRP.15.08.2025.p16426

[14] M. Grimland et al., "Cyberbullying victimization and suicide attempt among adolescents: A cross-national comparison", International Journal of Environmental Research and Public Health, 2025, vol. 22 (3), pp. 385 (1-14). Cyberbullying Victimization and Suicide Attempt Among Adolescents: A Cross-National Comparison | MDPI

[15] J. Casaña Mohedo et al., "Study of the Relationship Between Cyberbullying and Mental Health in Adolescents-A Systematic Review", Children, 2026, vol. 13 (3), pp. 367 (1-25). Study of the Relationship Between Cyberbullying and Mental Health in Adolescents—A Systematic Review | MDPI

[16] A. Denche-Zamorano et al., "Research on cyberbullying and suicide: a bibliometric analysis", Psychology in the Schools, 2025, vol. 62 (1), pp. 336-353.

[17] C. V. Swetha, S. Shaji, C. J. Kumar, "Review of State-of-the-Art Literature on Learning Techniques for Cyberthreat Detection on Online Social Media Networks" Journal of Engineering Science and Technology Review, 2025, vol. 18 (3). pp 152-169.

[18] A. Muneer, A. Alwadain, M. G. Ragab, and A. Alqushaibi, "Cyberbullying detection on social media using stacking ensemble learning and enhanced BERT", Information, 2023, vol. 14 (8), pp. 467 (1-20), Cyberbullying_Detection_on_Social_Media_Using_Stac.pdf

[19] S. Dudi, B. K. Singh, T. S. Ruprah, "Text Based Emotion Detection Using Deep Learning Technique" , Proceedings of the Multinova: First International Conference on Artificial Intelligence in Engineering, Healthcare and Sciences (ICAIEHS-2025). Springer Nature, 2025, pp. 100-121.

[20] O. Ezerceli, R. Dehkharghani, "Mental disorder and suicidal ideation detection", Journal of Computational Social Science, 2024, vol 7. pp. 2277–2307. Mental disorder and suicidal ideation detection from social media using deep neural networks | Journal of Computational Social Science | Springer Nature Link

[21] A. Dewani, M. A. Memon, S. Bhatti, "Cyberbullying detection: advanced preprocessing techniques and deep learning architecture for Roman Urdu data", Journal of big data, 2021, vol. 8 (1), pp. 160 (1-20).

[22] B. Fetaji, M. Ebibi, M.Fetaji, "Cybersecurity Forensics: A Systematic Literature Review", Editorial Board. Journal Of Computer Sciences and Mathematics (JCSM), 2024, vol. 1 (1), pp. 22-33.

[23] Z. Illési, "Digital Evidence Management for Organizational Legal Compliance",Interdisciplinary Description of Complex Systems: INDECS, 2025, vol. 23 (3), pp. 217-229.

Cyber Threats Targeting Human Health and Their Digital Expertise

Kamala Gurbanova[1], Khayala Abdulhuseynova[2]
[1,2]Institute of Information Technology, Baku, Azerbaijan
[1]*kemalewamil@gmail.com,* [2]*abdulxayala@gmail.com*

Abstract- Cyber threats targeting human health represent complex risks that impact an individual's biopsychological well-being in the digital environment. The research paper analyzes social and psychological consequences within the context of the human factor and investigates the correlation between cyberbullying and digital addiction. For the purpose of detecting cyber threats, intelligent analysis of textual data based on Transformer architectures such as BERT and RoBERTa, as well as RNN, LSTM, and BiLSTM neural network models, is examined. Furthermore, the intensity of risk dissemination and defense approaches in international practice are compared.

Keywords- cyber threat; bio-psychological well-being; hybrid deep learning models; BERT architecture; digital forensics.