Dövlətin Kibersuverenliyinə Çoxaspektli Yanaşma

Bəhruz Əliyev

Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası,
Bakı Dövlət Universiteti, Bakı, Azərbaycan
bahruz.work@gmail.com, bahruzaliyev@bsu.edu.az

***Xülasə*— Tədqiqat işində dövlətin kibersuverenliyinin təmin olunmasına çoxaspektli yanaşma irəli sürülür. Bu kontekstdə milli rəqəmsal müstəqillik, ağıllı şəhər infrastrukturları, yeni nəsil (post-quantum) kriptoqrafiya, süni intellekt əsaslı müdafiə mexanizmləri və insan faktorunun strateji rolu sistemli şəkildə təhlil edilir. Kadr çatışmazlığı, təşkilati mədəniyyət və maarifləndirmə səviyyəsi risklərin reallaşma ehtimalını müəyyən edən əsas amillər kimi qiymətləndirilir. Tədqiqat işində kibersuverenliyin gücləndirilməsi üçün milli rəqəmsal proqram və texnologiyalara, dayanıqlı kriptoqrafik transformasiyaya, təhlükəsiz infrastruktur dizaynına, süni intellekt ilə gücləndirilmiş müdafiəyə və insan kapitalının inkişafına əsaslanan konseptual yanaşma və prioritet istiqamətlər təklif olunur.**

Açar sözlər*— *kibersuverenlik; rəqəmsal müstəqillik; ağıllı şəhər; Əşyaların İnterneti; kibertəhlükəsizlik; post-quantum;, kriptoqrafiya; süni intellekt; kibermüdafiə; insan faktoru; kadr potensialı; kritik infrastruktur; milli avadanlıq; milli əməliyyat sistemi.

I. GİRİŞ

Son onilliklərdə rəqəmsal texnologiyaların sürətli inkişafı dövlətlərin suverenlik anlayışını epistemoloji və praktiki çərçivədə yenidən formalaşdırmışdır. İnformasiya məkanında sərhədlərin qeyri-müəyyən olması, transmilli platformaların dominant mövqeyi və qlobal data axınlarının intensivləşməsi milli təhlükəsizlik üçün yeni risk mühiti yaratmışdır. Müasir elmi ədəbiyyatda kibersuverenlik anlayışı dövlətin öz informasiya resursları üzərində nəzarət imkanlarını, milli rəqəmsal ekosistemin dayanıqlılığını və xarici texnoloji asılılıqların minimallaşdırılmasını ehtiva edən kompleks fenomen kimi xarakterizə olunur [1-2]. Bu məqalənin məqsədi kibersuverenliyə çoxölçülü yanaşmanı konseptual, texnoloji və institusional aspektləri təhlil etmək və elmi əsaslandırılmış inteqrativ model təklif etməkdir.

II. KONSEPTUAL VƏ NORMATİV ÇƏRÇİVƏ

Kibersuverenlik anlayışı müasir beynəlxalq münasibətlər və informasiya təhlükəsizliyi diskursunda dövlətlərin rəqəmsal mühit üzərində legitim səlahiyyətlərini ifadə edən fundamental konsepsiya kimi formalaşmaqdadır. Rəqəmsal məkanın transsərhəd xarakterinə baxmayaraq, dövlətlər milli təhlükəsizlik, ictimai sabitlik və strateji maraqların qorunması məqsədilə kiberməkanda normativ tənzimləmə və nəzarət mexanizmlərini genişləndirməyə çalışırlar. BMT-nin Hökumət Ekspertləri Qrupu (GGE - Groups of Governmental Experts) və Açıq İşçi Qrupu (OEWG - Open-ended Working Group) çərçivəsində aparılan müzakirələr kiberməkanda dövlət davranışları üçün norma və prinsiplərin formalaşdırılmasına yönəlmişdir və bu prosesdə dövlət suverenliyinin rəqəmsal müstəviyə tətbiqi legitim yanaşma kimi qəbul olunur [3].

Bununla yanaşı, İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (OECD - Organisation for Economic Co-operation and Development) və Avropa Şurası (Council of Europe) kimi beynəlxalq təşkilatların sənədlərində kibertəhlükəsizliyin idarə olunması milli məsuliyyət çərçivəsində təqdim edilir. Bu yanaşma kiberməkanda risklərin yalnız texniki problem kimi deyil, eyni zamanda hüquqi və institusional məsuliyyət sahəsi kimi qiymətləndirilməsini ön plana çıxarır. Normativ müstəvidə kibersuverenlik anlayışı informasiya təhlükəsizliyi siyasətləri, fərdi məlumatların qorunması haqqında qanunvericilik, kritik informasiya infrastrukturlarının mühafizəsinə dair hüquqi aktlar və data lokalizasiyası kimi mexanizmlər vasitəsilə konkretləşdirilir. Bu mexanizmlər dövlətin rəqəmsal mühitdə tənzimləyici rolunu gücləndirən institusional çərçivəni formalaşdırır.

Elmi ədəbiyyatda kibersuverenlik, informasiya təhlükəsizliyi, data suverenliyi və texnoloji müstəqillik anlayışları arasında sıx qarşılıqlı əlaqə mövcuddur [4]. Data suverenliyi konsepsiyası dövlətlərin öz yurisdiksiyasında formalaşan və saxlanılan məlumat axınlarına nəzarət etmək hüququnu vurğulayır və bu yanaşma kibersuverenliyin praktik təzahürlərindən biri kimi qiymətləndirilir. Texnoloji müstəqillik isə milli rəqəmsal ekosistemin xarici platformalardan, proqram təminatlarından və avadanlıq təchizatçılarından asılılıq səviyyəsinin azaldılmasını hədəfləyir. Bu kontekstdə kibersuverenlik təkcə hüquqi-normativ çərçivə ilə məhdudlaşmayan, həm də milli innovasiya ekosisteminin inkişafını stimullaşdıran strateji istiqamət kimi çıxış edir.

Konseptual baxımdan kibersuverenlik dövlətin rəqəmsal suverenliyinin institusional əsaslarını müəyyən etməklə yanaşı, onun beynəlxalq kiberməkanda davranış modellərinə də təsir göstərir. Dövlətlərin kiberməkanda fəaliyyətinə dair milli strategiyalar, kibertəhlükəsizlik doktrinaları və rəqəmsal inkişaf proqramları bu konsepsiyanın praktik implementasiya mexanizmlərini formalaşdırır. Bu sənədlərdə kibersuverenlik adətən dövlətin rəqəmsal infrastruktur üzərində nəzarət imkanlarının artırılması, milli məlumat resurslarının qorunması və kritik sistemlərin dayanıqlılığının təmin edilməsi kimi strateji məqsədlərlə əlaqələndirilir.

Eyni zamanda, kibersuverenliyin tətbiqi qlobal internetin fragmentasiyası risklərini artırmamalı, əksinə beynəlxalq hüquq normaları və çoxtərəfli əməkdaşlıq mexanizmləri ilə uzlaşdırılmış şəkildə həyata keçirilməlidir. Bu baxımdan kibersuverenlik milli maraqların qorunması şərti ilə, qlobal

DOI: 10.25045/cyber.gov.2026.10

rəqəmsal ekosistemi gözardı etmədən, münasibətlərdəki tarazlığın təmin olunması konsepsiyası kimi də qiymətləndirilə bilər.

III. MİLLİ RƏQƏMSAL MÜSTƏQİLLİK VƏ TEXNOLOJİ ASILILIQ PROBLEMİ

Milli rəqəmsal müstəqillik dövlətin əsas informasiya infrastrukturunun, kritik proqram təminatlarının və rəqəmsal xidmət ekosisteminin xarici platformalardan və texnoloji provayderlərdən asılılıq səviyyəsinin azaldılmasını nəzərdə tutur. Qloballaşmış İKT bazarında transmilli korporasiyaların dominant mövqeyi dövlətlərin məlumat axınları, bulud xidmətləri və platforma səviyyəli texnoloji həllər üzərində real nəzarət imkanlarını məhdudlaşdıra bilər. Bu asılılıq təkcə texniki risklər yaratmır, həm də hüquqi yurisdiksiya, məlumatların mühafizəsi və strateji qərarların icrasında institusional məhdudiyyətlər formalaşdırır. Xüsusilə transmilli bulud provayderlərinin data mərkəzlərinin coğrafi yerləşimi məlumatların yurisdiksiya xaricində saxlanılmasına səbəb olur ki, bu da milli qanunvericiliyin tətbiqi baxımından hüquqi qeyri-müəyyənliklər yaradır [5].

Milli rəqəmsal müstəqilliyin təmin olunmasında data suverenliyi konsepsiyası mühüm normativ çərçivə kimi çıxış edir. Data suverenliyi dövlətlərin öz yurisdiksiyasında formalaşan və saxlanılan məlumatlar üzərində hüquqi və texniki nəzarət mexanizmlərinin qurulmasını nəzərdə tutur. Bu baxımdan milli data mərkəzlərinin yaradılması, dövlət buludlarının (government cloud) formalaşdırılması və kritik informasiya sistemlərinin lokal infrastruktur üzərində yerləşdirilməsi kibersuverenliyin praktiki mexanizmləri kimi qiymətləndirilir. Tədqiqatlar göstərir ki, suveren bulud modelləri dövlət sektorunda məlumat təhlükəsizliyinin və əməliyyat dayanıqlılığının artırılmasına töhfə verir, eyni zamanda fövqəladə hallar zamanı informasiya xidmətlərinin fasiləsizliyini təmin edir [6].

Texnoloji asılılıq problemi yalnız infrastruktur səviyyəsi ilə məhdudlaşmır, eyni zamanda əməliyyat sistemləri, verilənlər bazası, idarəetmə sistemləri və təhlükəsizlik platformaları üzrə xarici vendorlara yüksək asılılıq, riskləri gücləndirir. Bu kontekstdə açıq mənbəli proqram təminatlarının strateji sahələrdə tətbiqi texnoloji müstəqilliyin gücləndirilməsi baxımından mühümdür. Açıq mənbə kodlu sistemlər təhlükəsizlik auditlərinin aparılmasını asanlaşdırır, potensial zəifliklərin aşkarlanmasında şəffaflığı artırır və yerli mütəxəssislərin texnoloji inkişafına şərait yaradır [7].

Milli rəqəmsal müstəqilliyin daha bir mühüm komponenti təchizat zənciri təhlükəsizliyidir. Kritik informasiya infrastrukturlarında istifadə olunan avadanlıq və proqram təminatlarının etibarlı mənbələrdən əldə edilməsi, sertifikatlaşdırma mexanizmlərinin tətbiqi ciddi əhəmiyət daşıyır. Qlobal təchizat zəncirlərinin mürəkkəbləşməsi fonunda avadanlıq (hardware) və proqram təminatı (software) səviyyəsində risklər müxtəlif hadisələrin təsiri ilə mümkündür. Məsələn süni intellektə olan tələb səbəbi ilə GPU istehsalında olan partlayış RAM kimi bəzi ehtiyat avadanlıqların qıtlaşmasına gətirib çıxardığını təchizatçıların cavablarından müşahidə etmək mümkündür. Eyni narahatçılıq fərqli siyasi proseslərdə də özünü biruzə verə bilər.

Ona görə də rəqəmsal müstəqillik üçün, gələcəkdə açıq mənbəli ƏS-i əsasında milli ƏS-in yaradılmasını kibersuverenliyimizə böyük təsir edə bilər. Milli avadanlıq istehsalına təkan vermək və onu stimullaşdırmaq, kritik avadanlıqlara və proqram təminatlarına olan ehtiyacları azaltmaq rəqəmsal müstəqilliyimizə xidmət edə bilər. Təbii ki, ilkin mərhələdə bu sahədə güclənməyə ehtiyacı olan digər ölkələrlə də güclərimizi birləşdirə bilərik. Buna misal olaraq, türk dilli ölkələrin öz İT güclərini birləşdirərək, kritik infrastrukturlar üçün, prioritet ola biləcək ƏS, proqram təminatları, şəbəkə və təhlükəsizlik avadanlıqlarının istehsalı gözdən keçirilə bilər. Hər il milli rəqəmsal müstəqilliyimiz üçün, istehsal gücümüzü artıra bilərik və diopazunumuzu genişləndirə bilərik.

Eyni zamanda nəzərə saxlamalıyıq ki, qlobal rəqəmsal ekosistemdən tam izolyasiya, innovasiya mübadiləsini zəiflədə bilər və texnoloji inkişafın sürətini azalda bilər. Ona görə də balansı da qorumaq mütləqdir.

IV. AĞILLI ŞƏHƏR EKOSİSTEMLƏRİ: RİSKLƏR VƏ DAYANIQLILIQ

Ağıllı şəhərlər, IoT əsaslı sensor şəbəkələr, böyük məlumat analitikası və əsasən bulud hesablamaları üzərində qurulmuş kompleks rəqəmsal ekosistemlərdir. Bu ekosistemlər nəqliyyatın intellektual idarə edilməsi, enerji paylanmasının optimallaşdırılması, ictimai təhlükəsizlik xidmətlərinin rəqəmsallaşdırılması və kommunal resursların səmərəli istifadəsi kimi funksional üstünlüklər yaradır. Lakin ağıllı şəhər infrastrukturlarının yüksək dərəcədə rəqəmsallaşdırılması hücum səthinin genişlənməsinə səbəb olur və bu mühitləri kibertəhlükəsizlik baxımından daha həssas edir.

Ağıllı şəhər sistemlərinin təhlükəsizlik zəifliklərı yalnız informasiya mühitində deyil, eyni zamanda fiziki müstəvidə də ciddi nəticələrə səbəb ola bilər. Məsələn, nəqliyyatın ağıllı idarəetmə sistemlərinə edilən kiberhücumlar yol hərəkətinin təhlükəsizliyini poza, enerji şəbəkələrinə müdaxilə isə genişmiqyaslı elektrik kəsintilərinə və sosial-iqtisadi itkilərə gətirib çıxara bilər. Elmi tədqiqatlarda qeyd olunur ki, kiber-fiziki sistemlərdə baş verən insidentlər klassik informasiya sistemlərindən fərqli olaraq birbaşa real dünya təsirləri yaratdığı üçün risklərin idarə olunması daha yüksək səviyyəli dayanıqlılıq mexanizmləri tələb edir [8].

Sistemlərin arxitektura səviyyəsində təhlükəsizlik tələblərinin nəzərə alınması, identifikasiya və autentifikasiya mexanizmlərinin gücləndirilməsi, şəbəkə seqmentasiyası və mikroseqmentasiya modellərinin tətbiqi hücumların yayılma potensialını əhəmiyyətli dərəcədə azalda bilər. Elmi ədəbiyyatda göstərilir ki, kritik sistemlərin şəbəkə səviyyəsində izolyasiyası və zero-trust arxitekturasının tətbiqi ağıllı şəhər ekosistemlərinin kiberdayanıqlılığını artıran effektiv mexanizmlər sırasında yer alır [9].

Eyni zamanda standartlara uyğun olmayan, təhlükəsizlik tələblərinə cavab verməyən İoT avadanlıqları həm quraşdırıldığı bölgəyə həm də quraşdırıldığı evdə vətəndaşı çətin vəziyyətə sala bilər. İnsan həyatına müxtəlif təsirləri ola bilər. Standartlara cavab verməyən İoT avadanlıqlarının, quraşdırıldığı yerlərdə, gizli müşahidə və səs yazısı daxil

olmaqla, kiberhücuma məruz qaldıqda müxtəlif narahatlıq və fəsadlar da törədə bilər. Ona görə də ölkəyə qəbul edilən İoT avadanlıqları üçün də standartlar olmalı və o standartlara cavab verən avadanlıqlar ölkə ərazisinə daxil ola bilməlidir. Əgər bu avadanlıqların qoşulduğu data mərkəzi varsa, onun ölkə ərazisində quraşdırılması və vətəndaşlara ölkə daxilindən xidmət göstərməsi nəzərdə tutula bilər. Ona görə də ağıllı şəhər və İoT avadanlıqlarını kibersuverenliyin möhkəmlənməsi üçün, diqqətə alınacaq bir peridmet olduğunu qeyd etmək mümkündür.

Normativ-institusional baxımdan ağıllı şəhər təhlükəsizliyinin təmin olunması çoxsəviyyəli idarəetmə mexanizmlərini tələb edir. Milli kibertəhlükəsizlik orqanları, özəl sektor tərəfdaşları və akademik institutlar arasında koordinasiyanın gücləndirilməsi kompleks risk mühitinin effektiv idarə olunmasına töhfə verir. Eyni zamanda, standartlaşdırma sahəsində ISO/IEC 27001, IEC 62443 və ağıllı şəhərlər üçün hazırlanmış beynəlxalq təhlükəsizlik çərçivələrinin tətbiqi texniki uyğunluğun və institusional məsuliyyətin sistemləşdirilməsinə imkan yaradır. Bu yanaşmalar ağıllı şəhər ekosistemlərinin yalnız funksional səmərəliliyini deyil, həm də uzunmüddətli təhlükəsizlik və dayanıqlılıq potensialını təmin edən əsas mexanizmlər kimi çıxış edir.

V. YENİ NƏSİL (POST-KVANT) KRİPTOQRAFİYA

Kvant hesablama texnologiyalarının sürətli inkişafı mövcud kriptoqrafik alqoritmlərin uzunmüddətli təhlükəsizliyinə dair fundamental çağırışlar formalaşdırır. Xüsusilə açıq açarlı kriptoqrafiyanın əsasını təşkil edən RSA, Diffie–Hellman və elliptik əyri kriptoqrafiyası (ECC - Elliptic-curve cryptography) kimi alqoritmlərin kvant kompüterlərində “Shor alqoritmi” vasitəsilə səmərəli şəkildə sındırıla bilmə potensialı kriptoqrafik infrastrukturun gələcək dayanıqlılığını sual altına alır. Elmi ədəbiyyatda qeyd olunur ki, “harvest now, decrypt later” (indi topla, sonra deşifrə et) ssenariləri dövlətlərin uzunmüddətli məxfi məlumatları üçün ciddi risk yaradır, çünki bu gün ələ keçirilən şifrəli məlumatlar gələcəkdə kvant hesablama imkanları genişləndikdə açıla bilər [10].

Post-kvant kriptoqrafiya (PQC - Post-Quantum Cryptography) klassik kompüterlərdə səmərəli işləyən, lakin kvant hücumlarına qarşı dayanıqlı hesab edilən kriptoqrafik alqoritmlərin hazırlanmasını hədəfləyir. Lattice-based (tor əsaslı), code-based (kod əsaslı), hash-based və multivariate polynomial əsaslı kriptoqrafik yanaşmalar elmi ictimaiyyət tərəfindən perspektivli istiqamətlər kimi qiymətləndirilir. ABŞ Milli Standartlar və Texnologiya İnstitutu (NIST) tərəfindən aparılan post-kvant kriptoqrafiya standartlaşdırma prosesi bu sahədə qlobal konsensusun formalaşdırılması baxımından mühüm mərhələ hesab olunur və milli kriptoqrafik strategiyaların elmi əsaslar üzərində qurulmasına imkan yaradır [10].

Dövlət səviyyəsində post-kvant kriptoqrafiyaya keçid yalnız texniki məsələ deyil, həm də institusional və normativ transformasiya tələb edən kompleks prosesdir. Mövcud kriptoqrafik infrastrukturun (PKI sistemləri, sertifikat mərkəzləri, təhlükəsiz rabitə protokolları) mərhələli şəkildə post-kvant alqoritmlərlə uyğunlaşdırılması uzunmüddətli planlaşdırma və risklərin idarə olunmasını tələb edir. Bu keçid prosesində hibrid kriptoqrafik modellərin (klassik + post-kvant alqoritmlərin paralel tətbiqi) istifadə olunması elmi ədəbiyyatda tövsiyə edilən praktik yanaşmalardan biridir və tranzit dövründə kriptoqrafik davamlılığın qorunmasına töhfə verir.

Kriptoqrafik suverenlik kontekstində milli kriptoalqoritmlərin hazırlanması və lokallaşdırılmış kriptoqrafik standartların tətbiqi kibersuverenliyin texnoloji dayaqlarını gücləndirən mühüm mexanizmlər kimi çıxış edir. Milli sertifikatlaşdırma mexanizmlərinin yaradılması, kriptoqrafik modulların və aparat təhlükəsizlik modullarının yerli audit və sertifikatlaşdırma prosedurlarından keçirilməsi dövlətin kriptoqrafik ekosisteminə nəzarət imkanlarını artırır [11]. Bu yanaşma həm xarici texnoloji asılılıqların azaldılmasına, həm də kritik sistemlərdə istifadə olunan kriptoqrafik həllərin etibarlılığının yüksəldilməsinə xidmət edir.

Eyni zamanda, post-kvant kriptoqrafiyanın tətbiqi performans, miqyaslana bilmə və resurs tələbləri baxımından yeni texniki çağırışlar yaradır. Bir çox PQC alqoritmləri klassik alqoritmlərlə müqayisədə daha böyük açar ölçülərinə və hesablamalı mürəkkəbliyə malikdir ki, bu da resurs məhdudiyyətli IoT cihazları və real vaxt rejimində işləyən kiber-fiziki sistemlər üçün əlavə optimallaşdırma ehtiyacları doğurur. Bu səbəbdən elmi tədqiqatlarda post-kvant kriptoqrafiyanın praktik implementasiyası üçün sistem arxitekturalarının adaptasiyası və optimallaşdırma mexanizmlərinin hazırlanması vacib istiqamətlərdən biri kimi göstərilir.

Post-kvant kriptoqrafiya yalnız gələcək texnoloji risklərə qarşı reaktiv cavab deyil, eyni zamanda dövlətlərin kibersuverenliyinin uzunmüddətli təminatı üçün proaktiv strateji investisiya kimi qiymətləndirilməlidir. Milli kriptoqrafik strategiyaların elmi əsaslar üzərində qurulması, standartlaşdırma prosesləri ilə uzlaşdırılması və kadr potensialının bu istiqamətdə gücləndirilməsi rəqəmsal təhlükəsizlik arxitekturasının davamlılığını təmin edən əsas şərtlər sırasında yer alır.

VI. SÜNİ İNTELLEKT ƏSASLI MÜDAFİƏ SİSTEMLƏRİ

Süni intellekt texnologiyalarının sürətli inkişafı kibertəhlükəsizlik sahəsində ənənəvi reaktiv müdafiə modellərindən proaktiv və adaptiv müdafiə arxitekturalarına keçidi mümkün etmişdir. Klassik imza-əsaslı təhlükəsizlik mexanizmləri yeni və naməlum hücum vektorlarını aşkarlamaqda məhdudiyyətlərə malik olduğu halda, maşın öyrənməsi və dərin öyrənmə əsaslı modellər şəbəkə trafiki, sistem loqları və istifadəçi davranışları üzərində kompleks nümunələri təhlil edərək anomaliyaların real vaxt rejimində müəyyən edilməsinə imkan yaradır [12]. Bu yanaşma xüsusilə sıfır-gün (zero-day) hücumlarının erkən mərhələdə aşkarlanması baxımından strateji üstünlük yaradır.

AI (Artificial intelligence – Süni intellekt) əsaslı IDS(Intrusion Detection System) / IPS ((Intrusion Prevention System) sistemlərinin effektivliyi böyük həcmli və heterogen məlumat mənbələrinin inteqrasiyasından asılıdır. Böyük məlumat analitikası ilə sinerji təşkil edən AI modelləri təhlükə

kəşfiyyatı (threat intelligence) məlumatlarını, şəbəkə telemetriyasını və son nöqtə davranışlarını vahid analitik çərçivədə birləşdirərək kontekstual risk qiymətləndirməsi aparmağa imkan verir. Elmi ədəbiyyatda vurğulanır ki, bu cür çoxmənbəli yanaşmalar təhlükəsizlik əməliyyat mərkəzlərinin (SOC) situasiya məlumatlılığını əhəmiyyətli dərəcədə artırır və insidentlərə reaksiya müddətini azaldır.

Bununla yanaşı, süni intellekt sistemlərinin özlərinin də yeni hücum səthləri yaratdığı nəzərə alınmalıdır. Adversarial learning, data poisoning və model evasion kimi texnikalar AI modellərinin təlim mərhələsində və istismar prosesində manipulyasiya edilməsinə şərait yarada bilər [13]. Xüsusilə adversarial nümunələr (adversarial examples) vasitəsilə maşın öyrənməsi modellərinin səhv qərarlar verməyə məcbur edilməsi kritik təhlükəsizlik sistemlərində ciddi risklər yaradır. Bu səbəbdən AI əsaslı müdafiə mexanizmlərinin etibarlı və izah edilə bilən (explainable AI) arxitekturalar üzərində qurulması elmi yanaşmalarda prioritet istiqamət kimi qeyd olunur.

AI əsaslı müdafiə sistemlərinin institusional tətbiqi normativ və etik məsələləri də gündəmə gətirir. Avtomatlaşdırılmış qərar qəbuletmə mexanizmlərinin şəffaflığı, yanlış pozitiv və yanlış neqativ qərarların idarə olunması, habelə fərdi məlumatların emalı ilə bağlı hüquqi tələblər AI əsaslı kibertəhlükəsizlik həllərinin legitimliyini müəyyən edən mühüm amillərdir. Dövlət səviyyəsində bu texnologiyaların tətbiqi zamanı hüquqi-normativ çərçivənin əvvəlcədən müəyyənləşdirilməsi və etik risklərin qiymətləndirilməsi institusional etimadın qorunması baxımından zəruridir.

Texniki baxımdan AI əsaslı müdafiə sistemlərinin dayanıqlılığının təmin olunması üçün modelin davamlı yenilənməsi, təlim məlumatlarının keyfiyyətinin təmin edilməsi və kiberdayanıqlı arxitekturaların (resilient architectures) tətbiqi vacibdir. Federativ öyrənmə (federated learning) kimi yanaşmalar mərkəzləşdirilməmiş mühitlərdə məlumat məxfiliyini qorumaqla AI modellərinin təkmilləşdirilməsinə imkan yaradır və bu da xüsusilə dövlət qurumları arasında məlumat paylaşımı məhdudiyyətlərinin mövcud olduğu hallarda praktik üstünlüklər yarada bilər.

Süni intellekt əsaslı müdafiə sistemləri kibertəhlükəsizlik arxitekturasında transformativ potensiala malik olmaqla yanaşı, yeni texnoloji və institusional risklər də formalaşdırır. Bu texnologiyaların kibersuverenlik kontekstində effektiv tətbiqi üçün AI əsaslı təhlükəsizlik həllərinin milli təhlükəsizlik strategiyaları ilə uzlaşdırılması, standartlaşdırma təşəbbüsləri ilə uyğunlaşdırılması və kadr potensialının bu sahədə sistemli şəkildə inkişaf etdirilməsi strateji əhəmiyyət kəsb edir.

VII. İNSAN FAKTORU VƏ KİBERMƏDƏNİYYƏT

Empirik tədqiqatlar göstərir ki, kiberinsidentlərin əhəmiyyətli hissəsi texniki zəifliklərdən deyil, məhz insan faktorundan qaynaqlanır. Sosial mühəndislik hücumları, phishing kampaniyaları, parol idarəetməsində yol verilən səhvlər və təhlükəsizlik prosedurlarına əməl olunmaması müasir informasiya sistemlərinin ən zəif halqalarından biri olaraq qalmaqdadır [14]. Bu kontekstdə insan faktorunun kibertəhlükəsizlik arxitekturasında kritik dəyişən kimi nəzərə alınması və sistemli şəkildə idarə olunması zəruridir.

Kibermədəniyyət anlayışı fərdlərin və təşkilatların informasiya təhlükəsizliyi ilə bağlı davranış modellərini, risk qavrayışını və normativ tələblərə uyğunluq səviyyəsini əhatə edir. Elmi ədəbiyyatda vurğulanır ki, texnoloji müdafiə mexanizmləri ilə yanaşı, təhlükəsizlik yönümlü davranış mədəniyyətinin formalaşdırılması uzunmüddətli perspektivdə kiberinsidentlərin qarşısının alınmasında daha dayanıqlı nəticələr verir. Dövlət sektorunda kibermədəniyyətin formalaşdırılması xüsusilə əhəmiyyətlidir, çünki dövlət qulluqçuları milli məlumat resursları və kritik sistemlərlə birbaşa təmasda olan əsas aktorlardır.

Davamlı təlim və sertifikatlaşdırma proqramları insan faktorundan irəli gələn risklərin azaldılmasında əsas institusional alətlərdən biri kimi çıxış edir. Kibertəhlükəsizlik sahəsində biliklərin sürətlə yenilənməsi fonunda bir dəfəlik təlimlər kifayət etmir; əksinə, davamlı peşəkar inkişaf mexanizmlərinin qurulması zəruridir. Simulyasiya əsaslı təlimlər, “phishing awareness” kampaniyaları və real insident ssenariləri üzrə təlimlər əməkdaşların təhlükə davranışlarını vaxtında tanıma və adekvat reaksiya vermə qabiliyyətini artırır. Elmi tədqiqatlar göstərir ki, davranış yönümlü təlim proqramları texniki təhlükəsizlik tədbirləri ilə sinerji yaratmaqla ümumi kiberdayanıqlılığı əhəmiyyətli dərəcədə yüksəldir.

İnsan faktorunun institusional səviyyədə idarə olunması kadr potensialının planlı şəkildə inkişaf etdirilməsini tələb edir. Milli kibertəhlükəsizlik ekosisteminin formalaşdırılması üçün yalnız texniki mütəxəssislərin deyil, eyni zamanda hüquqşünaslar, idarəetmə mütəxəssisləri və strateji planlaşdırma üzrə kadrların da rəqəmsal təhlükəsizlik sahəsində kompetensiyalarının artırılması vacibdir. Bu yanaşma kibersuverenliyin yalnız texniki deyil, həm də institusional və idarəetmə komponentlərini gücləndirən çoxşaxəli kadr siyasətinin formalaşdırılmasına xidmət edir.

Bununla yanaşı, kibermədəniyyətin formalaşdırılması yalnız dövlət sektorunun daxili məsələsi kimi məhdudlaşdırılmamalıdır. Cəmiyyətin geniş təbəqələrinin rəqəmsal savadlılığının artırılması milli səviyyədə kiber-dayanıqlılığın mühüm şərtlərindən biridir. İctimai maarifləndirmə kampaniyaları, təhsil sistemində informasiya təhlükəsizliyi mövzularının inteqrasiyası və özəl sektorla tərəfdaşlıq mexanizmləri insan faktorundan irəli gələn risklərin makrosəviyyədə azaldılmasına töhfə verə bilər. Beləliklə, kibermədəniyyətin formalaşdırılması dövlətin kibersuverenli-yinin institusional və sosial dayaqlarını gücləndirən strateji istiqamət kimi qiymətləndirilə bilər.

VIII. İNTEQRATİV MODEL VƏ STRATEJİ TƏKLİFLƏR

Məqalədə təklif olunan inteqrativ model kibersuverenliyin təmin olunmasına sistemli yanaşmanı əks etdirərək texnoloji, normativ-institusional və insan resursları komponentlərinin qarşılıqlı sinerjisinə əsaslanır. Bu model kibertəhlükəsizlik tədbirlərinin fragmentar şəkildə deyil, vahid milli təhlükəsizlik arxitekturası çərçivəsində əlaqələndirilmiş formada həyata keçirilməsini nəzərdə tutur. Elmi yanaşmalarda vurğulandığı kimi, yalnız texniki müdafiə mexanizmlərinin gücləndirilməsi

kibersuverenliyin uzunmüddətli təminatı üçün kifayət deyil; normativ tənzimləmə və institusional idarəetmə mexanizmləri ilə inteqrasiya olunmuş kompleks model tələb olunur.

Texnoloji komponent çərçivəsində milli rəqəmsal infrastrukturun dayanıqlılığının artırılması, kritik informasiya infrastrukturlarının qorunması, suveren bulud modellərinin tətbiqi və post-kvant kriptoqrafiya kimi yeni nəsil təhlükəsizlik texnologiyalarının mərhələli şəkildə inteqrasiyası prioritet istiqamətlər kimi müəyyən edilir. Bu istiqamətdə milli səviyyədə standartlaşdırma təşəbbüslərinin gücləndirilməsi, təhlükəsizlik arxitekturalarının vahid referens modellər əsasında qurulması və texnoloji risklərin davamlı monitorinqi tövsiyə olunur. Texnoloji komponentin effektivliyi onun normativ və insan resursları komponentləri ilə uzlaşdırılmasından birbaşa asılıdır.

Normativ-institusional komponent kibersuverenliyin hüquqi əsaslarının möhkəmləndirilməsini və dövlətin rəqəmsal mühitdə tənzimləyici rolunun institusionallaşdırılmasını nəzərdə tutur. Kibertəhlükəsizlik strategiyalarının, data suverenliyi ilə bağlı hüquqi aktların, kritik informasiya infrastrukturlarının mühafizəsinə dair normativ sənədlərin vahid strateji çərçivədə uyğunlaşdırılması sektorlararası koordinasiyanın gücləndirilməsinə xidmət edir. Bu kontekstdə milli səviyyədə kibertəhlükəsizlik üzrə koordinasiya mexanizmlərinin (məsələn, milli CERT/CSIRT strukturlarının gücləndirilməsi) institusional səlahiyyətlərinin dəqiqləşdirilməsi və onların dövlət qurumları, özəl sektor və akademik mühitlə qarşılıqlı fəaliyyət mexanizmlərinin formallaşdırılması vacibdir.

İnsan resursları komponenti inteqrativ modelin sosial-institusional dayağını təşkil edir və kadr potensialının sistemli şəkildə inkişaf etdirilməsini, kibermədəniyyətin formalaşdırılmasını və təşkilati davranış modellərinin təhlükəsizlik yönümlü transformasiyasını əhatə edir. Elmi ədəbiyyatda vurğulandığı kimi, texnoloji və normativ mexanizmlərin effektivliyi insan faktorunun yetkinlik səviyyəsindən əhəmiyyətli dərəcədə asılıdır. Bu səbəbdən milli kibertəhlükəsizlik ekosistemində ixtisaslaşmış kadr hazırlığı proqramlarının genişləndirilməsi, akademiya–sənaye–dövlət tərəfdaşlığının təşviqi və davamlı peşəkar inkişaf mexanizmlərinin institusionallaşdırılması strateji prioritet kimi çıxış etməlidir.

Strateji təkliflər çərçivəsində kibersuverenliyin təmin olunması üçün mərhələli yol xəritəsinin (roadmap) hazırlanması tövsiyə olunur. Bu yol xəritəsi qısamüddətli perspektivdə kritik infrastrukturun qorunması və risklərin azaldılması tədbirlərini, orta müddətli perspektivdə milli rəqəmsal infrastrukturun modernləşdirilməsi və post-kvant kriptoqrafiyaya keçid strategiyalarını, uzunmüddətli perspektivdə isə milli innovasiya ekosisteminin və texnoloji müstəqilliyin dayanıqlı şəkildə inkişaf etdirilməsini əhatə etməlidir. Hər mərhələ üçün ölçülə bilən performans göstəricilərinin müəyyən edilməsi strategiyanın monitorinqi və qiymətləndirilməsi baxımından mühüm əhəmiyyət kəsb edir.

Beynəlxalq əməkdaşlıq inteqrativ modelin xarici ölçüsünü təşkil edir və kibersuverenliyin qlobal rəqəmsal ekosistemlə uzlaşdırılmasını təmin edir. Dövlətlərarası informasiya mübadiləsi mexanizmləri, birgə təlimlər və standartlaşdırma təşəbbüslərində iştirak milli kibertəhlükəsizlik potensialının artırılmasına töhfə verə bilər. Bu baxımdan inteqrativ model milli maraqların qorunması ilə qlobal kibertəhlükəsizlik arxitekturasında konstruktiv iştirak arasında tarazlığın qorunmasına yönəlmiş strateji çərçivə kimi qiymətləndirilə bilər.

NƏTİCƏ

Aparılan elmi təhlil göstərir ki, kibersuverenlik müasir dövlətlərin milli təhlükəsizlik arxitekturasında çoxölçülü və dinamik xarakter daşıyan strateji anlayış kimi çıxış edir. Rəqəmsal transformasiyanın dərinləşməsi fonunda dövlətlərin informasiya mühitində üzləşdiyi risklər yalnız texniki xarakter daşımır, eyni zamanda hüquqi, institusional, iqtisadi və sosial ölçüləri əhatə edən kompleks təhlükəsizlik problemləri formalaşdırır. Bu baxımdan kibersuverenlik anlayışı təkcə kiberhücumlara qarşı müdafiə mexanizmlərinin mövcudluğu ilə məhdudlaşmır, həm də dövlətin rəqəmsal ekosistem üzərində effektiv idarəetmə və strateji nəzarət qabiliyyətini ifadə edir.

Məqalədə aparılan təhlillər göstərir ki, milli rəqəmsal müstəqillik, ağıllı şəhər infrastrukturlarının təhlükəsizliyi, post-kvant kriptoqrafiya yanaşmalarının inteqrasiyası, süni intellekt əsaslı müdafiə mexanizmlərinin institusionallaşdırılması və insan faktorunun sistemli şəkildə idarə olunması kibersuverenliyin əsas struktur komponentlərini təşkil edir. Bu komponentlərin hər biri ayrı-ayrılıqda əhəmiyyət kəsb etsə də, onların real effektivliyi yalnız inteqrativ və koordinasiyalı şəkildə tətbiq olunduğu təqdirdə təmin edilə bilər. Parçalanmış və sektorlararası koordinasiyadan məhrum təhlükəsizlik yanaşmaları müasir kiber təhdid mühitinin mürəkkəbliyinə adekvat cavab verməkdə məhdudiyyətlərə malikdir.

Eyni zamanda, kibersuverenliyin təmin olunması statik deyil, davamlı transformasiya tələb edən proses kimi qiymətləndirilməlidir. Texnoloji mühitin sürətli dəyişməsi, yeni hücum vektorlarının meydana çıxması və geosiyasi kontekstin dinamikası dövlətlərin kibertəhlükəsizlik strategiyalarını periodik olaraq yenidən nəzərdən keçirməsini zəruri edir. Bu baxımdan milli kibertəhlükəsizlik strategiyalarının adaptiv xarakter daşıması, risk əsaslı idarəetmə modellərinin tətbiqi və elmi tədqiqatlarla praktiki siyasət formalaşdırılması arasında institusional körpülərin qurulması xüsusi əhəmiyyət kəsb edir.

Nəticə etibarilə, kibersuverenliyin milli təhlükəsizlik strategiyalarında prioritetləşdirilməsi rəqəmsal mühitdə dayanıqlı inkişafın təmin olunmasının əsas şərtlərindən biri kimi çıxış edir. Dövlətlərin bu istiqamətdə atacağı ardıcıl və elmi əsaslandırılmış addımlar yalnız cari kiber risklərin azaldılmasına deyil, həm də uzunmüddətli perspektivdə milli rəqəmsal suverenliyin və strateji dayanıqlılığın möhkəmləndirilməsinə töhfə verəcəkdir.

ƏDƏBİYYAT

[1] T. Maurer, Cyber Mercenaries, Cambridge University Press, 2018.

[2] J. Nye, “Deterrence and Dissuasion in Cyberspace,” International Security, vol. 41, no. 3, pp. 44–71, 2017.

[3] United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Report, 2021.

[4] R. Deibert, Black Code: Surveillance, Privacy, and the Dark Side of the Internet, Signal, 2013.

[5] OECD, Digital Security Risk Management, OECD Publishing, 2022.

[6] ENISA, Cybersecurity for Smart Cities, European Union Agency for Cybersecurity, 2021.

[7] E. S. Raymond, The Cathedral and the Bazaar, O'Reilly Media, 2001.

[8] A. Zanella et al., "Internet of Things for Smart Cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32, 2014.

[9] ISO/IEC 27001:2022, Information Security Management Systems.

[10] NIST, Post-Quantum Cryptography Standardization, 2023.

[11] D. J. Bernstein et al., Post-Quantum Cryptography, Springer, 2009.

[12] S. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[13] I. Goodfellow et al., "Explaining and Harnessing Adversarial Examples," ICLR, 2015.

[14] Verizon, Data Breach Investigations Report, 2024

A Multifaceted Approach to State Cyber Sovereignty

Bahruz Aliyev

Azerbaijan Cybersecurity Organizations Association,

Baku State University, Baku, Azerbaijan

Abstract— In the research work, a multi-aspect approach to ensuring the state's cyber sovereignty is put forward. In this context, national digital independence, smart city infrastructures, next-generation (post-quantum) cryptography, artificial intelligence–based defense mechanisms, and the strategic role of the human factor are systematically analyzed. Human resource shortages, organizational culture, and the level of awareness are assessed as the main factors determining the probability of risk realization. In the research work, a conceptual approach and priority directions based on national digital programs and technologies, sustainable cryptographic transformation, secure infrastructure design, AI-enhanced defense, and the development of human capital are proposed for strengthening cyber sovereignty.

Keywords— cyber sovereignty; digital independence; smart city; Internet of Things, cybersecurity; post-quantum; cryptography; artificial intelligence; cyber defense; human factor; human resources; critical infrastructure; national equipment; national operating system.