Rəqəmsal Fərqlərin Dövlətin Kibersuverenliyinə Yaratdığı Təhlükələrin və Risklərin Analizi

Rəsmiyyə Mahmudova[1], Çinarə İsayeva[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*rasmahmudova@gmail.com*, [2]*chinaraasgarova@mail.ru*

***Xülasə*— Rəqəmsal fərqlərin artması dövlətlərin kibersuverenliyinə fundamental təhdid yaradan amil kimi çıxış edir. İnfrastruktur, texnologiya və fərdi rəqəmsal bacarıqlardakı bərabərsizliklər kiberhücumlara qarşı milli müdafiə sistemlərini zəiflədir, milli təhlükəsizlik və iqtisadi sabitlik üçün risklər yaradır. Bu fərqlər dövlətlərin öz rəqəmsal ekosistemlərini müstəqil idarə etmə imkanlarını məhdudlaşdırır, xarici texnoloji asılılığı dərinləşdirir və informasiya müharibələrində strateji zəifliklər doğurur. Məqalədə rəqəmsal uçurumun kibersuverenlik kontekstində yaratdığı təhlükələrin analizi aparılır və rəqəmsal bərabərsizliyin aradan qaldırılması vasitəsilə milli kiberdayanıqlılığın artırılması üçün konseptual strateji yanaşmalar təhlil olunur.**

Açar sözlər*— *kibersuverenlik; rəqəmsal fərqlər; süni intellekt; risk analizi; rəqəmsal bərabərsizlik; alqoritmik suverenlik.

I. GİRİŞ

Müasir dövrdə rəqəmsal texnologiyaların cəmiyyətin bütün sferalarına sürətli inteqrasiyası dövlət idarəçiliyi və milli təhlükəsizlik paradiqmalarını köklü şəkildə dəyişmişdir. Kiberməkan artıq sadəcə texnoloji platforma deyil, dövlətlərin öz siyasi və iqtisadi maraqlarını qoruduğu beşinci strateji domen hesab olunur. Bu kontekstdə "kibersuverenlik" anlayışı - dövlətin öz rəqəmsal infrastrukturu üzərində müstəqil nəzarəti həyata keçirmək və kənar müdaxilə olmadan milli rəqəmsal siyasətini müəyyən etmək hüququ kimi ön plana çıxır [1]. Lakin qlobal şəbəkənin mərkəzsizləşdirilmiş təbiəti ilə dövlətlərin suverenlik iddiaları arasındakı ziddiyyət yeni çağırışlar yaradır.

Dövlətlərin kibersuverenliyini təhdid edən ən kritik faktorlardan biri "rəqəmsal fərqlər" (digital divide) fenomenidir. Ənənəvi olaraq rəqəmsal fərqlər sadəcə internetə çıxış imkanları arasındakı bərabərsizlik kimi izah edilsə də, müasir tədqiqatlarda bu anlayış daha geniş - texnoloji asılılıq, kiber-savadlılıq və innovasiya potensialı arasındakı uçurum kimi xarakterizə olunur [2]. Jan van Dijk-in qeyd etdiyi kimi, rəqəmsal bərabərsizlik fərdlərin və dövlətlərin texnologiyadan istifadə keyfiyyətinə və ondan əldə etdikləri strateji dividendlərə birbaşa təsir göstərir [3].

Texnoloji cəhətdən inkişaf etmiş dövlətlər rəqəmsal ekosistemdə standartları müəyyən etdiyi halda, rəqəmsal uçurumun digər tərəfində qalan dövlətlər "rəqəmsal asılılıq" və ya "rəqəmsal müstəmləkəçilik" riski ilə üzləşirlər [4]. Bu asılılıq xarici proqram təminatı və avadanlıq istehsalçılarının dövlətin daxili informasiya mühitinə gizli təsir imkanlarını artırır. Beynəlxalq Telekommunikasiya İttifaqının (ITU) hesabatlarında vurğulanır ki, rəqəmsal savadlılıq və infrastruktur boşluqları dövlətin kiberdayanıqlılığını zəiflədərək, onu həm kiber-cinayətkarlıq, həm də xarici dövlətlərin informasiya əməliyyatları qarşısında müdafiəsiz qoyur [5].

Müasir mərhələdə süni intellekt (Sİ) texnologiyalarının inkişafı rəqəmsal fərqləri daha da dərinləşdirərək "alqoritmik qeyri-bərabərlik" problemini ortaya çıxarmışdır. Sİ sahəsində texnoloji resurslara və böyük verilənlərə (Big Data) malik olan dövlətlər digər ölkələrin informasiya məkanı üzərində mütləq üstünlük qazanırlar. Bu, həm avtomatlaşdırılmış kiberhücumların (məsələn, Sİ əsaslı fişinq və ya zərərli proqramlar), həm də "deepfake" texnologiyaları vasitəsilə həyata keçirilən dezinformasiya kampaniyalarının dövlətin kibersuverenliyinə təsirini kritik dərəcədə artırır [6]. Beləliklə, Sİ sahəsindəki fərqlər dövlətlərin kiber-müdafiə qabiliyyəti ilə yanaşı, həm də onların texnoloji müstəqilliyini birbaşa təhdid edir [7]."

II. DÖVLƏTİN KİBERSUVERENLİYİ ANLAYIŞI, MAHİYYƏTİ

Suverenlik anlayışı beynəlxalq münasibətlər nəzəriyyəsinin əsas kateqoriyalarından biridir. Klassik yanaşmaya görə, suverenlik dövlətin öz ərazisi daxilində ali hakimiyyətə malik olması və beynəlxalq münasibətlərdə digər dövlətlərdən hüquqi baxımdan asılı olmaması deməkdir. Bu anlayışın sistemli nəzəri əsaslandırılması XVI əsrdə Jan Boden tərəfindən verilmiş, daha sonra isə Vestfal sülhü (1648) ilə beynəlxalq münasibətlər sisteminin fundamental prinsipi kimi möhkəmlənmişdir [8,9]. Müasir beynəlxalq hüquqda isə suveren bərabərlik prinsipi BMT Nizamnaməsində öz əksini tapmışdır [10].

Suverenlik anlayışı Vestfal sülhündən sonra beynəlxalq münasibətlərin əsas prinsipi kimi formalaşıb və indi rəqəmsal sahədə də öz əksini tapır. Zinovyeva və Şitkov (2026) qeyd edirlər ki, rəqəmsal suverenlik dövlətin təhlükəsizliyini və iqtisadi potensialını müəyyən edən əsas amillərdən biridir. Müəlliflər qeyd edirlər ki, Rusiya və Çin milli internet seqmentini qorumağı əsas prioritet sayır, ABŞ isə uzun müddət interneti qlobal və sərhədsiz məkan kimi qəbul edib.

XXI əsrdə rəqəmsal transformasiya nəticəsində suverenliyin tətbiq sahəsi genişlənmiş və informasiya-kommunikasiya texnologiyaları (İKT) mühiti dövlət hakimiyyətinin yeni ölçüsünə çevrilmişdir. Rəqəmsal məkanın transsərhəd xarakteri klassik ərazi əsaslı suverenlik modelini

DOI: 10.25045/cyber.gov.2026.44

çətinləşdirsə də, dövlətlər öz yurisdiksiyalarını rəqəmsal infrastruktura, məlumatlara və kiberməkana şamil etməyə çalışırlar. Bu kontekstdə “kibersuverenlik” anlayışı formalaşmışdır.

Kibersuverenlik ümumi şəkildə dövlətin öz milli informasiya infrastrukturuna, rəqəmsal platformalarına və məlumat axınlarına nəzarət etmək hüququ və imkanları kimi izah olunur. Bəzi müəlliflər bu anlayışı beynəlxalq hüququn mövcud prinsiplərinin kiberməkana tətbiqi kimi qiymətləndirirlər [11]. Xüsusilə, BMT-nin Hökumət Ekspertləri Qrupunun (GGE) 2013 və 2015-ci illər hesabatlarında dövlət suverenliyinin və ondan irəli gələn prinsiplərin İKT mühitinə də şamil olunduğu vurğulanmışdır [12].

Eyni zamanda, kibersuverenlik anlayışı müxtəlif siyasi və mədəni kontekstlərdə fərqli şəkildə şərh olunur. Çin akademik və siyasi diskursunda “internet suverenliyi” termini dövlətin öz milli internet seqmenti üzərində tam nəzarət hüququnu ifadə edir [13]. Avropa İttifaqında isə “rəqəmsal suverenlik” daha çox strateji muxtariyyət, məlumatların qorunması və texnoloji asılılığın azaldılması ilə əlaqələndirilir [14]. ABŞ akademik diskursunda isə uzun müddət internetin qlobal və açıq məkan kimi qəbul edilməsi üstünlük təşkil etmiş, dövlət nəzarətinin genişlənməsi tənqidi qiymətləndirilmişdir [15].

Kibersuverenliyin nəzəri əsaslarının mühüm komponentlərindən biri də yurisdiksiya məsələsidir. Rəqəmsal məlumatların fiziki olaraq müxtəlif ölkələrin serverlərində saxlanılması və transsərhəd məlumat axınlarının artması dövlətlərin hüquqi səlahiyyətlərinin sərhədlərini mürəkkəbləşdirir. Bu vəziyyət beynəlxalq münasibətlərdə “rəqəmsal təhlükəsizlik dilemması”nın formalaşmasına səbəb olur, çünki dövlətlərin müdafiə məqsədli tədbirləri digər dövlətlər tərəfindən təhdid kimi qəbul edilə bilər [16].

Beləliklə, kibersuverenlik klassik suverenlik anlayışının rəqəmsal transformasiyası kimi çıxış edir. O, bir tərəfdən beynəlxalq hüququn mövcud prinsiplərinə əsaslanır, digər tərəfdən isə rəqəmsal texnologiyaların transsərhəd və qeyri-ərazi xarakteri səbəbindən yeni normativ və institusional mexanizmlərin formalaşdırılmasını zəruri edir. Bu nəzəri çərçivə rəqəmsal fərqlərin dövlətlərin kibersuverenliyinə təsirini və yaranan riskləri təhlil etmək üçün konseptual əsas yaradır.

III. Rəqəmsal Fərqlər: Mahiyyəti və Strukturu

Rəqəmsal fərqlər, müasir dövrdə dövlətlərin kibersuverenliyinə qarşı ən ciddi təhdidlərdən biri olaraq çıxış edir. Rəqəmsal uçurum, yalnız internetə çıxış imkanları ilə əlaqəli deyil, həm də dövlətlərin texnoloji asılılığı, kiber-savadsızlıq və innovasiya potensialı arasındakı fərqlərlə bağlıdır [17,18]. Rəqəmsal uçurumun bu çoxölçülü xarakteri (texnoloji, təhsil və innovativ) dövlətin kiberməkandakı manevr imkanlarını məhdudlaşdıran struktur baryerlərə çevrilir.

Bu kontekstdə “rəqəmsal fərqlər” (digital divide) anlayışı İKT-yə çıxış, onlardan istifadə imkanları və rəqəmsal bacarıqlar baxımından mövcud olan fərqləri ifadə edir. İlk mərhələdə bu anlayış əsasən internetə fiziki çıxış imkanları ilə əlaqələndirilsə də, sonrakı tədqiqatlarda onun daha kompleks və çoxsəviyyəli xarakter daşıdığı göstərilmişdir [17,19].

Müasir ədəbiyyatda rəqəmsal fərqlər adətən üç səviyyədə təhlil olunur: infrastruktura çıxış fərqləri, istifadə və bacarıq fərqləri, əldə olunan sosial-iqtisadi nəticələrdə fərqlər. J. van Dijk rəqəmsal fərqlərin yalnız texnoloji çatışmazlıqla deyil, sosial struktur, təhsil səviyyəsi və iqtisadi resurslarla sıx bağlı olduğunu vurğulayır. Bu yanaşma rəqəmsal bərabərsizliyin yalnız texniki deyil, həm də institusional və struktur xarakter daşıdığını göstərir [20].

Texnoloji inkişaf səviyyələri arasındakı fərqlər dövlətlərin qlobal rəqəmsal iqtisadiyyatda mövqeyini müəyyən edən əsas amillərdəndir. İnkişaf etmiş ölkələr yüksək sürətli internet infrastrukturu, genişzolaqlı şəbəkələr, data mərkəzləri və bulud texnologiyaları sahəsində üstünlüyə malikdirlər. Beynəlxalq Telekommunikasiya İttifaqının (ITU) hesabatlarına görə, yüksək gəlirli ölkələrdə internet istifadə səviyyəsi 90 %-dən çox olduğu halda, aşağı gəlirli ölkələrdə bu göstərici 30–40 % civarındadır [21,22]. Bu fərq rəqəmsal xidmətlərə çıxış və texnoloji innovasiyaların tətbiqi imkanlarında da özünü göstərir.

Rəqəmsal fərqlərin struktur komponentlərindən biri infrastruktur amilidir. Fiber-optik şəbəkələrin yayılması, 5G texnologiyasına çıxış və milli data mərkəzlərinin mövcudluğu dövlətlərin rəqəmsal müstəqilliyini və kibersuverenlik imkanlarını birbaşa təsirləndirir. İnfrastruktur zəifliyi xarici texnoloji platformalardan və xidmət təminatçılarından asılılığı artırır. Bu isə milli məlumatların saxlanması, emalı və qorunması sahəsində risklər yaradır [21,22].

İnsan kapitalı rəqəmsal fərqlərin digər mühüm komponentidir. Rəqəmsal bacarıqların səviyyəsi, STEM təhsili, elmi-tədqiqat potensialı və innovasiya mühiti dövlətlərin rəqəmsal transformasiyaya adaptasiya qabiliyyətini müəyyən edir. OECD və Dünya Bankının tədqiqatları göstərir ki, yüksək rəqəmsal bacarıqlara malik ölkələr rəqəmsal iqtisadiyyatdan daha çox fayda əldə edir və texnoloji asılılıq riski daha aşağı olur [23,24]. Əksinə, aşağı ixtisaslı əmək bazarı və zəif innovasiya ekosistemi rəqəmsal fərqləri dərinləşdirir.

İnnovasiya potensialı da rəqəmsal fərqlərin əsas struktur göstəricilərindəndir. Qlobal İnnovasiya İndeksi (WIPO) məlumatlarına əsasən, yüksək gəlirli ölkələr patent fəaliyyəti, elmi nəşrlər və yüksək texnologiyalı məhsul ixracı sahəsində üstün mövqedədirlər. Bu üstünlük onların qlobal texnoloji dəyər zəncirində dominant mövqe tutmasına və rəqəmsal platformalar üzərində nəzarət imkanlarının genişlənməsinə şərait yaradır [25].

İnkişaf etmiş və inkişaf etməkdə olan ölkələr arasında rəqəmsal fərqlər xüsusilə data iqtisadiyyatı və platforma iqtisadiyyatı kontekstində daha aydın görünür. Qlobal rəqəmsal platformaların böyük hissəsi məhdud sayda ölkədə yerləşir və bu vəziyyət rəqəmsal asılılıq münasibətləri formalaşdırır. UNCTAD-ın hesabatlarında qeyd olunur ki, inkişaf etməkdə olan ölkələr rəqəmsal iqtisadiyyatda əsasən istehlakçı rolunda çıxış edir, yüksək əlavə dəyər isə inkişaf etmiş ölkələrdə cəmləşir [26].

Müasir dövrdə rəqəmsal fərqlərin yeni ölçülərindən biri süni intellekt (Sİ) savadlılığıdır. Bu anlayış yalnız texniki

bacarıqları deyil, həm də etik, hüquqi və strateji bilikləri əhatə edir. Süni intellekt texnologiyalarına çıxış və onların istifadəsi bacarıqları bərabər paylanmadığı üçün dövlətlər və sosial qruplar arasında yeni bərabərsizlik formaları yaranır [27].

Son tədqiqatlarda vurğulanır ki, Sİ savadlılığı yüksək olan ölkələr və sosial qruplar rəqəmsal iqtisadiyyatdan daha çox fayda götürür, bazar məlumatlarını daha effektiv analiz edir və texnoloji innovasiyalardan strateji üstünlük qazanırlar [27,26]. Əksinə, Sİ savadlılığı aşağı olan qruplar alqoritmik qərarvermə sistemlərinə daha çox asılı vəziyyətdə qalır və bu, həm iqtisadi, həm də sosial qeyri-bərabərliyi dərinləşdirir [24].

Maliyyə bazarları kontekstində aparılan araşdırmalar göstərir ki, süni intellekt savadlılığı investorların riskləri qiymətləndirmə və qərarvermə keyfiyyətinə birbaşa təsir göstərir. Sİ savadlılığı olmayan investorlar rəqəmsal platformalara kor asılılıqla yanaşır, bu isə onların strateji muxtariyyətini zəiflədir. Bu baxımdan, Sİ savadlılığının artırılması yalnız texniki təlim deyil, həm də etik və hüquqi çərçivələrin formalaşdırılması ilə bağlıdır [24].

Beləliklə, süni intellekt savadlılığı rəqəmsal fərqlərin yeni struktur komponenti kimi qəbul edilməlidir. Onun inkişafı kibersuverenliyin möhkəmlənməsi, rəqəmsal iqtisadiyyatda bərabər iştirak və sosial ədalətin təmin olunması üçün strateji əhəmiyyət daşıyır [24,28].

IV. RƏQƏMSAL FƏRQLƏRİN YARATDIĞI TƏHLÜKƏLƏR VƏ RİSKLƏR

Rəqəmsal fərqlər dövlətlərin kibertəhlükəsizlik sahəsindəki dayanıqlılığını zəiflədən, onların rəqəmsal ekosistemlərindəki bərabərsizlikləri daha da dərinləşdirən və kibermüdafiə sahəsində strateji boşluqlar yaradan amildir [1-3]. J. van Dijk-in qeyd etdiyi kimi, rəqəmsal bərabərsizlik yalnız texniki çatışmazlıq deyil, həm də sosial-texniki sistemin zəifliyidir [1]. Bu bərabərsizliklər aşağıdakı təhdid vektorları vasitəsilə kibersuverenliyə risklər yaradır:

A. Kibersavadsızlıq və informasiya müdafiəsinin zəifləməsi

Dövlətlər arasındakı rəqəmsal savadlılıq uçurumu milli kibermüdafiə qabiliyyətinə birbaşa mənfi təsir göstərir. Dövlət və cəmiyyət səviyyəsində rəqəmsal savadlılığın aşağı olması kibertəhlükəsizlik protokollarının düzgün tətbiq edilməməsi, informasiyanın qorunması sahəsində sistemli boşluqların formalaşması və dövlət qurumlarında zəif kibermüdafiə mexanizmlərinin yaranması ilə xarakterizə olunur [30]. Bu şəraitdə insan faktoru rəqəmsal təhlükəsizlik arxitekturasının ən zəif həlqəsinə çevrilir.

Beynəlxalq Telekommunikasiya İttifaqının (ITU) hesabatlarında qeyd edilir ki, rəqəmsal savadlılıq və infrastruktur boşluqları dövlətin kibermüdafiə qabiliyyətini zəiflədir və onu həm kiber-cinayətkarlıq, həm də xarici dövlətlərin informasiya əməliyyatları qarşısında müdafiəsiz qoyur [5,21,22]. Rəqəmsal savadlılıq səviyyəsinin aşağı olması nəticəsində insan faktoru üzərindən həyata keçirilən hücumlar – xüsusilə fişinq və sosial mühəndislik üsulları – texniki müdafiə mexanizmlərini asanlıqla neytrallaşdıra bilir. Nəticə etibarilə bu vəziyyət dövlətin kibersərhədlərini qorumaq və öz rəqəmsal siyasətini müstəqil şəkildə müəyyən etmək qabiliyyətini məhdudlaşdıraraq kibersuverenliyin funksional zəifləməsinə gətirib çıxarır [3,30].

B. Texnoloji asılılıq və təchizat zənciri riskləri

İnnovasiya potensialındakı fərqlər dövlətlərin xarici texnoloji provayderlərdən asılılığını artırır [5], bu da uzunmüddətli strateji zəiflik yaradır. Texnoloji cəhətdən inkişaf etmiş dövlətlər rəqəmsal ekosistemdə standartları və texniki normaları müəyyən etdikcə, digər ölkələr normativ və texnoloji baxımdan asılı mövqedə qalırlar. Nəticədə xarici proqram təminatçıları və avadanlıq istehsalçıları dövlətlərin daxili informasiya mühitinə dolayı təsir imkanları əldə edirlər [4,5].

Bu vəziyyət xüsusilə inkişaf etməkdə olan dövlətlər üçün “rəqəmsal müstəmləkəçilik” və “rəqəmsal asılılıq” risklərini gücləndirir [6,7,29]. Milli proqram təminatı və avadanlıq istehsalının zəifliyi informasiya infrastrukturu üzərində tam nəzarətin təmin edilməsini çətinləşdirir və dövlətin daxili informasiya mühitində nəzarət imkanlarını azalda bilər. Xarici mənşəli texnologiyaya yerləşdirilən gizli “arxa qapılar” və ya təchizat zənciri hücumları məlumat sızması və manipulyasiya riskini artırır [30].

SolarWinds supply chain attack hadisəsi göstərdi ki, dövlət qurumlarının istifadə etdiyi proqram təminatına təchizat mərhələsində sızma bütün milli informasiya mühitini kənar nəzarətə açа bilər [12]. Bu presedent rəqəmsal asılılığın milli təhlükəsizlik ölçüsünü aydın şəkildə ortaya qoyur.

C. Süni intellekt və alqoritmik qeyri-bərabərlik riskləri

Süni intellekt (Sİ) texnologiyalarının inkişafı rəqəmsal fərqləri daha da dərinləşdirir [28,31,32]. Sİ resurslarına və böyük məlumat bazalarına malik dövlətlər strateji üstünlük əldə edir, digərləri isə alqoritmik qərarların obyektinə çevrilirlər [31,32]. Bu vəziyyət dövlətlərarası kibertəhlükəsizlik balansını pozur və rəqəmsal sərhədlərin qorunmasını çətinləşdirir [31,32]. Məlumat hegemonluğu şəraitində alqoritmik sistemlər üzərində nəzarət itirildikdə, milli təhlükəsizlik infrastrukturu xarici texnoloji sistemlərdən asılı qalır.

Müasir mərhələdə milli Böyük Dil Modellərinin yoxluğu dövlətin qərarvermə mexanizmlərində xarici texnoloji asılılığı kritik həddə çatdırır. Dövlət əhəmiyyətli məlumatların və hətta dövlət sirri təşkil edən informasiyaların xarici Sİ platformaları tərəfindən emalı, verilənlərin kənar serverlərdə saxlanılması və alqoritmik qərəzlilik vasitəsilə strateji qərarların manipulyasiyası birbaşa kibersuverenliyə təhdididir. Alqoritmik suverenliyin təmin olunmaması, dövlətin rəqəmsal mühitdə öz maraqlarını qorumaq qabiliyyətini xarici proqram təminatçılarının etik və siyasi filtrindən asılı vəziyyətə salır.

Sİ əsaslı sistemlər avtomatlaşdırılmış kiberhücumlar, fişinq hücumları və zərərli proqramların digər dövlətlərə qarşı geniş istifadəsini mümkün edir. Eyni zamanda deepfake texnologiyalarının geniş yayılması dezinformasiya və psixoloji əməliyyatların təsir gücünü artırır [32]. Nəticədə dövlətlərin daxili siyasi sabitliyinə və beynəlxalq münasibətlərinə birbaşa təsir göstərilir.

D. İqtisadi və struktur qeyri-bərabərlik

Rəqəmsal inkişaf səviyyəsindəki fərqlər iqtisadi rəqabət qabiliyyətində də asimmetriya yaradır [25,26,33]. İnkişaf etmiş dövlətlər rəqəmsal infrastrukturu və innovasiya ekosistemini gücləndirməklə qlobal iqtisadi sistemdə üstün mövqe əldə edirlər, inkişaf etməkdə olan dövlətlər isə rəqəmsal transformasiyanın üstünlüklərindən tam istifadə edə bilmirlər.

Bu vəziyyət sosial bərabərsizliyin artmasına, əmək bazarında struktur dəyişikliklərin qeyri-bərabər paylanmasına və rəqəmsal uçurumun daha da dərinləşməsinə səbəb olur [3,18,19]. Nəticədə rəqəmsal fərqlər yalnız texnoloji deyil, həm də sosial-iqtisadi təhlükəsizlik problemi kimi çıxış edir.

NƏTİCƏ

Aparılan təhlil göstərir ki, rəqəmsal fərqlər müasir dövrdə yalnız inkişaf göstəricisi deyil, dövlətin kibersuverenliyinə təsir edən struktur təhlükəsizlik amilidir. İnfrastruktur, texnoloji imkanlar və insan kapitalı sahəsindəki qeyri-bərabərliklər dövlətlərin rəqəmsal mühit üzərində effektiv nəzarət imkanlarını məhdudlaşdırır və qərarvermə müstəqilliyini zəiflədir.

Rəqəmsal asılılığın artması xarici texnoloji platformalardan və proqram təminatından asılılığı dərinləşdirir, bu isə təchizat zənciri risklərini və informasiya təhlükəsizliyi boşluqlarını gücləndirir. SolarWinds supply chain attack hadisəsi bu asılılığın milli təhlükəsizlik müstəvisində konkret nəticələr doğura biləcəyini nümayiş etdirmişdir.

Eyni zamanda süni intellekt və böyük məlumat texnologiyalarının qeyri-bərabər inkişafı alqoritmik üstünlük formalaşdıraraq rəqəmsal fərqləri geosiyasi balans amilinə çevirir. Beləliklə, rəqəmsal fərqlər dövlətin kibersuverenlik funksiyasını zəiflədən və milli təhlükəsizlik arxitekturasında çoxölçülü risklər yaradan sistemli faktordur.

Bu tədqiqat çərçivəsində aşağıdakı strateji istiqamətlər prioritet hesab edilə bilər.

1) *Rəqəmsal insan kapitalının gücləndirilməsi* - kibertəhlükəsizlik və Sİ sahəsində ixtisaslaşmanın artırılması, dövlət qurumlarında davamlı təlim mexanizmlərinin formalaşdırılması.

2) *Milli texnoloji dayanıqlılığın artırılması* - kritik informasiya infrastrukturunda xarici asılılığın azaldılması və yerli texnoloji ekosistemin inkişafı.

3) *Normativ və beynəlxalq koordinasiya* - kibertəhlükəsizlik üzrə beynəlxalq standartlara inteqrasiyanın gücləndirilməsi və transmilli risklərin kollektiv idarə olunması.

4) *İnnovasiya ekosisteminin gücləndirilməsi* - startapların dəstəklənməsi, yerli texnologiya istehsalının stimullaşdırılması və dövlət-özəl tərəfdaşlıqlarının genişləndirilməsi.

5) *Süni intellekt savadlılığının artırılması* - texniki biliklərlə yanaşı etik və hüquqi çərçivələrin formalaşdırılması, alqoritmik bərabərsizliyin azaldılması.

MİNNƏTDARLIQ

Tədqiqatın ideya müəllifi akademik Rasim Əliquliyevə təşəkkür edirəm.

ƏDƏBİYYAT

[1] M. Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge, U.K.: Polity Press, 2017.
[2] J. S. Nye Jr., *The Future of Power*. New York, NY, USA: PublicAffairs, 2011, pp. 113–151.
[3] J. van Dijk, *The Digital Divide*. Cambridge, U.K.: Polity Press, 2020.
[4] N. N. Schia, "The cyber sovereignty and the digital divide: Analysis of the international politics of cyberspace," *European Journal of International Security*, vol. 3, no. 2, pp. 161–179, 2018.
[5] International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2024 Report*. Geneva, Switzerland: ITU Publications, 2024.
[6] J. S. Radu, "The strategic implications of artificial intelligence for cyber sovereignty," *Journal of International Affairs*, vol. 73, no. 1, pp. 101–118, 2023.
[7] D. G. Webster, "Artificial intelligence and the digital divide: Challenges for national security," *Global Security Review*, vol. 5, no. 3, pp. 45–62, 2024.
[8] J. Bodin, *Six Books of the Commonwealth*, M. J. Tooley, Trans. Oxford, U.K.: Basil Blackwell, 1955 (original work published 1576).
[9] S. D. Krasner, *Sovereignty: Organized Hypocrisy*. Princeton, NJ, USA: Princeton University Press, 1999.
[10] United Nations, *Charter of the United Nations*, 1945. [Online]. Available: https://www.un.org/en/about-us/un-charter
[11] M. N. Schmitt, Ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, U.K.: Cambridge University Press, 2017.
[12] United Nations General Assembly, "Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security," A/70/174, Jul. 22, 2015.
[13] B. Fang, "Cyber sovereignty: Reflection on the development of internet governance," *China International Studies*, no. 4, pp. 14–26, 2011.
[14] European Commission, "Shaping Europe's digital future," Brussels, Belgium, 2020. [Online]. Available: https://digital-strategy.ec.europa.eu
[15] J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World*. Oxford, U.K.: Oxford University Press, 2006.
[16] L. Eriksson and G. Giacomello, "The information revolution, security, and international relations: (IR)relevant theory?" *International Political Science Review*, vol. 27, no. 3, pp. 221–244, 2006.
[17] Organisation for Economic Co-operation and Development (OECD), *Understanding the Digital Divide*. Paris, France: OECD Publishing, 2021.
[18] P. Vassilakopoulou and E. Hustad, "Bridging digital divides: A literature review and research agenda," *Information Systems Frontiers*, vol. 25, pp. 955–969, 2021.
[19] P. DiMaggio *et al*., "Digital inequality: From unequal access to differentiated use," *Social Inequality Review*, 2021.
[20] J. van Dijk, *The Digital Divide*, Cambridge, UK: Polity Press, 2020. www.researchgate.net/publication/336775102_The_Digital_Divide
[21] International Telecommunication Union (ITU), *Measuring Digital Development: Facts and Figures 2023*. Geneva, Switzerland, 2023.
[22] International Telecommunication Union (ITU), *Facts and Figures 2024: Global Connectivity and 5G Coverage*. Geneva, Switzerland, 2024.
[23] Organisation for Economic Co-operation and Development (OECD), *Digital Divide in Education*. Paris, France: OECD Publishing, 2023.
[24] World Bank, *Digital Progress and Trends Report*. Washington, DC, USA, 2023.
[25] World Intellectual Property Organization (WIPO), *Global Innovation Index 2025*. Geneva, Switzerland, 2025.

[26] United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2024*. Geneva, Switzerland, 2024.
[27] Organisation for Economic Co-operation and Development (OECD), *Artificial Intelligence Policy Observatory*. Paris, France, 2021.
[28] Stanford University, *AI Index Report 2024*. Stanford, CA, USA, 2024.
[29] L. Newman *et al*., "Cybersecurity and developing countries: Risks and opportunities," *Journal of Cyber Policy*, vol. 7, no. 3, pp. 345–367, 2022.
[30] A. Bada and M. A. Sasse, "Cybersecurity awareness and training in developing nations," *Computers & Security*, vol. 102, pp. 102–118, 2021.
[31] M. Brundage *et al*., "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation," *arXiv preprint* arXiv:1802.07228, 2018.
[32] R. Chesney and D. K. Citron, "Deep fakes: A looming challenge for privacy, democracy, and national security," *California Law Review*, vol. 107, pp. 1753–1819, 2019.
[33] D. M. West, *Going Digital: The Challenges of AI and Cybersecurity for Developing Countries*. Washington, DC, USA: Brookings Institution, 2020.

Analysis of Threats and Risks Posed by Digital Divides To State Cyber sovereignty

Rasmiyya Mahmudova, Chinara Isayeva

Institute of Information Technology Baku, Azerbaijan

Abstract— The increasing digital divide acts as a factor posing fundamental threats to the cyber sovereignty of states. Inequalities in infrastructure, technology, and individual digital skills weaken national defense systems against cyber attacks, creating risks for national security and economic stability. These disparities limit the ability of states to independently manage their digital ecosystems, deepen foreign technological dependence, and create strategic vulnerabilities in information warfare. This paper analyzes the threats posed by the digital divide in the context of cyber sovereignty and examines conceptual strategic approaches to enhancing national cyber-resilience by eliminating digital inequality.

Keyword— cyber sovereignty; digital divide; artificial intelligence; risk analysis; digital inequality; algorithmic sovereignty.