Dövlətin Kibersuverenliyinin Ümumarxitektur Prinsipləri və Funksional Komponentləri: Problemlər və Konseptual Yanaşmalar

Fərhad Yusifov
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
farhadyusifov@gmail.com

***Xülasə*— Dövlət idarəçiliyində rəqəmsal transformasiyalar və süni intellekt texnologiyalarının tətbiqi dövlətin kibersuverenliyinin təmin edilməsi baxımından yeni çağırışlar, təhdidlər və risklər yaradır. Tədqiqat işində dövlətin kibersuverenliyinin arxitektur prinsipləri və təklif olunan modellər araşdırılır. Aparılan tədqiqatlarda dövlətin kibersuverenliyinin səviyyələr üzrə strukturlaşdırılmasına dair fərqli yanaşmalar mövcuddur. Bu yanaşmalar əsasən texnoloji, infrastruktur, məlumatların idarə olunması və geosiyasi təsirlərin nəzərə alınması kimi komponentləri əhatə edir. Tədqiqat işində dövlətin kibersuverenliyinin təmin edilməsi üçün konseptual model təklif edilmişdir. Təklif olunan yanaşma texnoloji, idarəetmə və sosial səviyyələrdən ibarətdir və bu səviyyələr birlikdə ölkənin kibersuverenlik ekosistemini formalaşdırır.**

Açar sözlər*— *kibersuverenlik; dövlət idarəçiliyi; dövlətin kibersuverenliyi; rəqəmsal texnologiyalar; süni intellekt.

I. GİRİŞ

Rəqəmsal transformasiyalar və süni intellektin tətbiqi dövlət idarəçiliyində ciddi dəyişikliklərə səbəb olmuşdur. Rəqəmsal transformasiyaların nəticələri dövlət idarəçiliyi ilə yanaşı bir çox digər sahələrə təsir göstərir. Son tədqiqatlar göstərir ki, dünyada baş verən geosiyasi gərginliklər, müharibələr, qarşıdurmalar fonunda kibersuverenlik aktual məsələlərdən birinə çevrilmişdir [1,2]. Məsələn, Amerika Birləşmiş Ştatları (ABŞ) və Çin arasında Tayvanla bağlı gərginlik yüksək texnologiyalı yarımkeçiricilər bazarının istehsalının təxminən 70%-ə nəzarət etmək istəyindən irəli gəlir [1,3]. Kibersuverenlik anlayışı dünyada və Avropada geniş yayılmasına baxmayaraq aparılan ədəbiyyat icmalı bu sahədə biliklərin hələ də sistemli olmadığını göstərir [2,4,5]. Kibersuverenlik dövlətin rəqəmsal infrastrukturunu, məlumat və informasiya axınlarını müstəqil olaraq müəyyən etmək və idarə etmək imkanına malik olmasıdır [6,7]. Bu konsepsiya təkcə kiberhücumlardan qorunma və şəbəkələrin etibarlılığının təmin edilməsi kimi texnoloji aspektləri deyil, həm də rəqəmsal məkanda öz müqəddəratını təyinetmə hüququ ilə bağlı siyasi, iqtisadi və sosial aspektləri əhatə edir. Başqa sözlə, kibersuverenlik dövlətin rəqəmsal resurslarına, o cümlədən, verilənlərə, infrastruktura və proqram təminatına nəzarət etmək imkanlarının olması ilə ifadə olunur. Dövlətin əsas fəaliyyət sahələrinin rəqəmsallaşması, dövlət suverenliyinin təmin olunması baxımından yeni təhdidlər və risklər yaradır. Rəqəmsallaşma, texnoloji transformasiyalar şəraitində ölkələrin müstəqilliyini qoruması kontekstində rəqəmsal texnologiyalar dağıdıcı potensiala malikdir.

Hazırda dövlətlərin apardığı siyasətə nəzər yetirdikdə aydın olur ki, suverenliyin təmin olunması və qorunması məsələləri ilə bağlı gündəmdə ciddi dəyişikliklər müşahidə olunur. Bu dəyişikliklər rəqəmsal kommunikasiyaların eksterritorial xarakteri ilə müəyyən olunur. Qlobal rəqəmsal kommunikasiya məkanının mövcudluğu ənənəvi suverenliyin ərazi məhdudiyyətlərini aradan qaldırmağa və xaricdən dövlətin suveren siyasi və iqtisadi sistemlərinin fəaliyyətinə əhəmiyyətli dərəcədə təsir göstərməyə imkan verir. Texnoloji cəhətdən inkişaf etmiş dövlətin suverenliyi bu gün artıq ərazi sərhədlərinə, müstəqil ictimai-siyasi və iqtisadi kursun mövcudluğuna görə deyil, daha çox xarici geosiyasi aktorların dövlətin və cəmiyyətin əsas fəaliyyət sahələrinə rəqəmsal müdaxiləsinə qarşı sistemli şəkildə müqavimət göstərə bilmək qabiliyyəti ilə müəyyən olunur. Ədəbiyyat analizi göstərir ki, ayrı-ayrı ölkə təcrübələrinə istinadən kibersuverenliklə bağlı yanaşmalar, modellər olsa da, bu sahədə tədqiqatlar hələ də ilkin mərhələdədir. Bəzi tədqiqatlarda dövlətin kibersuverenliyin təmin olunması üçün müxtəlif arxitekturalar və modellər təklif olunmuşdur. Bu yanaşmalar əsasən infrastruktur, məlumatların idarə olunması və hüquqi tənzimləmələrlə məhdudlaşır. Baxılan işdə dövlətin kibersuverenliyinin arxitektur prinsipləri və funksional komponentləri araşdırılır.

II. DÖVLƏTİN KİBERSUVERENLİYİNƏ DAİR BAXIŞLAR

Rəqəmsal transformasiyaların nəticələri dövlət idarəçiliyi, elm, təhsil, səhiyyə, biznes və digər bir çox sahələrə təsir göstərir. Milli informasiya məkanları ətrafında rəqəmsal sərhədlər formalaşır, informasiya-kommunikasiya resursları və infrastruktur getdikcə daha çox eksterritorial xüsusiyyət qazanır, xarici təsir imkanları genişlənir, hakimiyyətin legitimlik prinsipləri dəyişir və digər mühüm proseslər müşahidə olunur. Bu baxımdan dövlətin kibersuverenliyi aktual tədqiqat istiqamətlərindən biri hesab olunur. Son araşdırmalar göstərir ki, hazırda kibersuverenliyin təmin olunması məsələlərinə həsr olunmuş tədqiqatların sayı sürətlə artmaqdadır [2,8-10]. Əksər tədqiqatlarda bu fenomen əsasən müəyyən bir sahə ilə əlaqədar şəkildə araşdırılır. Avropa üçün bu termin əsasən fundamental hüquqların qorunması, məlumatların məxfiliyi və xarici texnologiyalardan asılılığın azaldılması ətrafında formalaşmışdır [11-13]. Siyasi və hüquqi müstəvidə dövlət rejimləri, internet senzurası, məlumatların

DOI: 10.25045/cyber.gov.2026.13

filtrasiyası müxtəlif məqsədlərin, o cümlədən, ictimai asayişin qorunması, nəzarətin, siyasi sabitliyin, dövlət və ictimai təhlükəsizliyin təmin edilməsi, suverenliyin qorunması və s. həyata keçirilməsi üçün tədqiq olunur. Aparılan tədqiqatlar kibersuverenliyin olmaması ilə bağlı risklərin azaldılmasına və bu sahədə "verilənlərin suverenliyi", "dövlətin İKT infrastrukturuna nəzarət suverenliyi", "platforma kimi dövlət" və s. konsepsiyaların işlənməsinə yönəlmişdir. Kibersuverenliyin əhəmiyyəti texnoloji transformasiyaların qlobal xarakteri və rəqəmsal texnologiyaların eksterritoryal olması ilə əlaqədar olaraq daha da artır. Müasir geosiyasi müstəvidə əsas gərginlik mənbələri çox vaxt texnoloji münaqişələrlə bağlıdır. Suveren milli fəzaya informasiya müdaxiləsi və ya müdaxiləyə cəhdlər, qlobal texnoloji şirkətlərin ictimai-siyasi və sosial-iqtisadi proseslərdə artan rolu, qlobal rəqəmsal kommunikasiya məkanında informasiya qarşıdurmasının güclənməsi, eləcə də, milli siyasi və iqtisadi institutlara yönələn kiberhücumlar bu tendensiyanın başlıca təzahürlərindəndir. Eyni zamanda, süni intellekt (Sİ) və proqram təminatı sahəsindəki inkişaf rəqəmsal mühiti güclü şəkildə siyasi platformaya çevirir və aşağıdakı yanaşmaları irəli sürməyə imkan verir [8]:

- dövlətlərin kiberməkanda müxtəlif maraqlarının mövcudluğu. Məsələn, inkişaf etmiş dövlətlərin internetin ayrı-ayrı seqmentlərini nəzarətə götürmək niyyətləri.
- dövlətlər, onların tərəfdarları və rəqibləri arasında müxtəlif səviyyələrdə qarşıdurmanın olması;
- informasiya müharibələrinin iqtisadi təzyiq, sanksiya və şantaj alətinə çevrilməsi;
- kriptovalyutalar və mərkəzləşdirilməmiş maliyyə alətlərini yaymağa çalışan şəbəkə təşkilatlarının ənənəvi dövlət suverenliyi üçün birbaşa təhlükə yaratması.
- Bəzi dövlətlərin maraqlarının müəyyən rəqəmsal korporasiyaların maraqları ilə birləşməsi, "rəqəmsal imperiyaların" yaranması.

Son zamanlar kibersuverenlik konsepsiyası iki istiqamətdə daha çox diqqət çəkir. Birinci istiqamət iqtisadi monopoliya və intellektual mülkiyyətlə bağlıdır ki, bu da əsasən yarımkeçirici istehsalını, 5G infrastrukturunu və verilənlərlə Sİ-in sui-istifadəsini hədəfləyir [1,14,15]. İkinci istiqamət isə daha çox kibermüharibələrlə bağlıdır [16,17]. Kibersuverenlik bir dövlətin məlumatlarını, infrastrukturunu və rəqəmsal resurslarını, xüsusilə də xarici təsirdən, kibertəhdidlərdən və xarici nəzarətdən qorumaq, tənzimləmək və idarə etmək bacarığını ifadə edir. Hazırda kibersuverenlik həqiqətəndə Avropa Birliyi (AB) ölkələri və ABŞ kimi bəzi dövlətlərin əsas prioritetləri arasındadır [5,18-20]. Bu kontekstdə kibertəhlükəsizlik kibersuverenliyin qorunması üçün mühüm komponentlərdən biri kimi çıxış edir. Dövlətlər vətəndaşlarını, iqtisadiyyatlarını və idarəetmə strukturlarını kiberhücumlardan, casusluqdan və rəqəmsal məkandakı müstəqilliklərinə təhdid yarada biləcək pozuntulardan qorumaq üçün güclü kibertəhlükəsizlik tədbirləri həyata keçirməlidirlər.

Hazırda *Google, Youtube, Facebook, Twitter, Instagram* kimi qlobal informasiya-kommunikasiya platformalarından milyardlarla insan istifadə edir. Bu platformalar insanların ölkələri, tarixi, mədəniyyəti və dəyərləri barədə düşüncələrini dəyişərək milli kimlik və mənəvi dəyərlərə təsir göstərmək gücündədir. Onlar həmçinin siyasi və iqtisadi institutların fəaliyyətinə təsir edərək, dövlət idarəçiliyinin fəaliyyət istiqamətini xarici qüvvələrin maraqlarına uyğun şəkildə dəyişə bilirlər [6]. Bu problemlər qloballaşan dünyada sosial-texnoloji reallığın formalaşması şəraitində dövlətin suverenliyini qorumaq baxımından qarşılaşa biləcəyi mümkün çağırışları müəyyənləşdirməsinin olduqca vacib olduğunu göstərir [6,8].

Suverenlik ənənəvi olaraq mübahisəli hüquqi və siyasi kateqoriya olub və kiberməkanda suverenliklə bağlı müzakirələr davam edir. Qloballaşma və rəqəmsal texnologiyalar suverenlik üçün xüsusilə ciddi problemlər yaradır. Texnoloji transformasiyalar kontekstində kiberməkan suverenliyinin təmin olunması üçün əlverişli sayılmayan bir mühit kimi təsəvvür edilirdi. Onun sərhədləri yoxdur və digər fiziki məkanlarla kəsişərək coğrafi sərhədlərin təsirini aradan qaldırır. Son oniliklərdə rəqəmsal dünyada suverenlik məsələsi hələ də mübahisələrə səbəb olur və geniş auditoriyalarda müzakirə mövzusu olaraq qalmaqdadır.

III. DÖVLƏTİN KİBERSUVERENLİK EKOSİSTEMİ: TƏHLÜKƏLƏR VƏ RİSKLƏR

Rəqəmsal texnologiyaların sürətli inkişafı və kibertəhdidlərin artması şəraitində milli maraqların şəbəkədə qorunması məsələsi getdikcə daha da aktuallaşır. Kibersuverenlik dövlətin rəqəmsal infrastrukturunu, verilənlərini və informasiya axınlarını müstəqil şəkildə müəyyənləşdirmək və idarə etmək imkanlarını əks etdirir. Avropa Birliyi ölkələrində suverenlik əsas hüquqların qorunması, məlumatların məxfiliyi və xaricidən gətirilən texnologiyalardan asılılığın azaldılması çərçivəsində formalaşdırılır [13,21,22]. Digər tərəfdən, ABŞ modelində kibersuverenlik yeni bazarların açılması və innovasiya əsaslı inkişafa yönəldilmiş və istehsaldan texnologiyaların istehlakına qədər böyük rəqəmsal platformaların və ekosistemin inkişafına üstünlük verilmişdir [13,23].

İnkişaf etmiş ölkələr, o cümlədən, AB kibersuverenlik üçün mübarizə aparsa da, hazırda qlobal verilənlər landşaftında Çin və ABŞ dominantlıq edir [24]. Çin dövlətyönümlü modeli qəbul etmiş, suverenliyə texno-millətçi yanaşmalar əsasında özünün siyasətini formalaşdırmışdır. Çinin qlobal verilənlər üzərində dominatlıq etmək məqsədi, həssas verilənlərin xarici dövlətlərə axınının qarşısını almaq, böyük verilənlərin toplanması və emalı üçün Sİ modellərini sürətlə geniş miqyasda tətbiq etməkdən ibarətdir. Nəticə etibarilə, Çin mərkəzləşdirilmiş internet idarəçiliyinin inkişafına fokuslanmış, sosial platformalarda paylaşılan kontent üzərində nəzarəti artırmasına, əksəriyyəti bu və ya digər formada dövlətin nəzarətində olan platformaların inkişaf etdirilməsində maraqlıdır. Ümumilikdə Çin hökuməti güclü nəzarət mexanizmini milli təhlükəsizliyin təmin olunması ilə əsaslandıran dövlət siyasəti kimi təqdim edir [25]. Lakin bazar iqtisadiyyatında baş verən böhranlar suverenliklə bağlı yanaşmaların hələ də formalaşma mərhələsində oluğunu göstərir. Məsələn, "Böyük Səd" (Great Firewall) artıq tam şəkildə tətbiq olunur, amma regiondan kənara məlumat axınlarını tənzimləyən qaydaların praktikada həyata

keçirilməsində hələ də çətinliklər mövcuddur [13]. ABŞ isə texnologiya nəhənglərinin bulud xidmətləri və Sİ sahəsindəki tədqiqatlarındakı dominantlığı ilə qabaqcıl mövqeyini qoruyur [5]. Amazon (AWS), Google və Microsoft kimi şirkətlər dünya üzrə bulud infrastrukturunun mühüm hissəsin idarə edir, eyni zamanda bu Avropa məkanında verilənlərin konfidensiallığı və təhlükəsizliyi məsələlərinə dair narahatlıqları artırır [4,5]. ABŞ texnoloji dominantlığını qoruyub saxlamaq üçün qabaqcıl hesablama texnologiyalarının ixracına nəzarət etməkdə davam edir [26]. Nəticə etibarilə, ABŞ kibersuverenliyinin əsas xüsusiyyətlərindən biri onun ekspansionist xarakteri, texnoloji asılılıq vasitəsilə müxtəlif bölgələr üzərində nəzarəti artırmaq və geosiyasi rəqiblərinə qarşı alyansın lideri olmaq səyləridir [27]. Bu güc göstərcisi AB-nin rəqəmsal məhsullar, xidmətlər, infrastruktur və intellektual mülkiyyətin 80%-dən çoxunu xarici ölkələrdən asılı olduğunu əks etdirir və Avropanın həqiqi kibersuverenlik əldə etməyə çalışarkən nə dərəcədə ciddi problemlə üz-üzə olduğunu bir daha göstərmiş olur [5,11]. Bu tədqiqatda ABŞ, AB ölkələri, Çin və Rusiya kimi dövlətlərin təcrübəsində kibersuverenliyə dair müxtəlif yanaşmalar təhlil olunur. Cədvəl 1-də dövlətlərin kibersuverenli dair strategiyaları müqayisəli şəkildə verilmişdir.

CƏDVƏL 1. DÖVLƏTLƏRİN KİBERSUVERENLİK STRATEGİYALARI

Ölkə	Strategiya / model	Əsas hədəf	Hüquqi sənədlər	Texnoloji yanaşma
AB	“Vətəndaş mərkəzli”, tənzimləyici, avtonom model	Fərdi məlumatların qorunması və rəqəmsal hüquqlar	Verilənlərin mühafizəsi (GDPR), Süni intellekt, Verilənlərin idarə olunması	“Suveren Bulud” (Gaia-X), asılılığın azaldılması
ABŞ	“Açıq Bazar”/ Liberal, çoxtərəfli	İqtisadi üstünlük və innovasiya fəaliyyətində sərbəstlik	Bulud infrastrukturu, Korporativ özünütənzimləmə	Silikon Vadisi nəhəngləri (Big Tech) vasitəsilə qlobal təsir imkanları
Çin	“Kibersuverenlik” / Dövlət mərkəzli, avtoritar model	Milli təhlükəsizlik və daxili informasiya nəzarəti	“Böyük Səd”, məlumat təhlükəsizliyi qanunu	Yerli texnologiya nəhəngləri (Baidu, Alibaba, Tencent) və qapalı ekosistem
Rusiya	“Suveren İnternet”/ müdafiə məqsədli, avtoritar model	Qlobal şəbəkədən avtonomluq və senzura	“Suveren RuNet” qanunu, verilənlərin lokalizasiyası	Xarici platformaların bloklanması, milli DNS sisteminin tətbiqi

Müqayisəli analiz nəticələri göstərir ki, ABŞ, AB ölkələri, Çin və Rusiya kimi dövlətlərin təcrübəsində kibersuverenliyə dair müxtəlif yanaşmalar vardır [24-29]. Kibersuverenliyin təmin olunmasını zəruri edən bir sıra təhdidlər, risklər və çağırışlar nəzər alınmalıdır. Əsas təhdidlərdən biri böyük informasiya axınlarını idarə edən rəqəmsal platformaların (Google, Amazon, Yahoo, Apple) əksəriyyətinin ABŞ-da yerləşməsi və onların fəaliyyətində geosiyasi neytrallıq prinsiplərinin nəzərə alınmamasıdır. Texnoloji monopolyanın olması kibersuverenliyə çox ciddi təhdiddir. Bir digər mühüm amil nəhəng platformalar geniş təsir imkanlarına malik olsalar da, dezinformasiyanın yayılmasına görə faktiki olaraq heç bir hüquqi məsuliyyət daşımırlar. Geosiyasi qarşıdurmalar fonunda təkcə rəqəmsal platformalar deyil, həmçinin ödəniş sistemləri (Visa, MasterCard, American Express) və istifadəçilər barədə məlumat toplanması məqsədilə istifadə olunan smartfonlar (Məsələn, Iphone) belə bir növ silaha çevrilir. Partnyor ölkələrlə, tərəfdaşlarla ünsiyyət qurmaq və dövlətin kibersuverenliyini təmin etmək arasında tarazlıq, balansın saxlaması vacibdir. Çin, Rusiya, Cənubi Koreya və Hindistan kimi ölkələr artıq bu istiqamətdə irəliləyirlər. Digər tərəfdən, aydındır ki, hazırda İnternetin və informasiya təhlükəsizliyinin beynəlxalq səviyyədə effektiv şəkildə tənzimlənməsi mümkün deyil. Bu sahədə aparılan bütün danışıqlar və təşəbbüslər ABŞ, Çin, Rusiya, AB tərəfindən sistemli şəkildə pozulur. Kompromisli alternativ həll kimi, texnoloji monopoliyanın istisna edildiyi və heç bir aktorun hökmranlıq edə bilmədiyi balanslaşdırılmış şəkildə texnologiyalardan istifadə təklif oluna bilər. Bunun üçün texnologiyanı təqdim edən və alan tərəf üçün bərabər imkanlar yaradılmalıdır. Bu isə beynəlxalq əməkdaşlıq və texnologiya transferinin daha ədalətli və davamlı əsaslar üzərində qurulmasına imkan verər.

IV. DÖVLƏTİN KİBERSUVERENLİYİN ARXİTEKTUR PRİNSİPLƏRİ VƏ FUNKSİONAL KOMPONENTLƏRİ

Bir sıra tədqiqat işlərində kibersuverenliyin müxtəlif səviyyələr üzrə strukturlaşdırılmasına dair fəqli yanaşmalar vardır. Müxtəlif tədqiqatlarda kibersuverenliyin təmin edilməsi məqsədilə fərqli arxitekturalar və konseptual modellər irəli sürülmüşdür [7,13,30,31]. Bu yanaşmalar əsasən milli informasiya infrastrukturunun qorunması, məlumatların lokallaşdırılması, şəbəkə üzərində nəzarətin gücləndirilməsi və kibertəhlükəsizliyin artırılması kimi istiqamətləri əhatə edir. Bununla yanaşı, belə modellərin tətbiqi qlobal internetin açıq və sərhədsiz təbiəti ilə müəyyən ziddiyyətlər yaradır və beynəlxalq əməkdaşlığın əhəmiyyətini daha da ön plana çıxarır.

Təklif olunan arxitekturalar, konseptual modellər əsasən infrastruktur, məlumatların idarə olunması, tənzimləyici dövlət orqanı və geosiyasi təsirlər kimi aspektləri əhatə edir. Beynəlxalq təcrübə nəzərə alınaraq dövlətin kibersuverenliyinin təmin olunması üçün konseptual model Şəkil 1-də verilmişdir [13].

Şəkil 1. Dövlətin kibersuverenliyinin konseptual modeli

İlk növbədə, infrastruktur səviyyə ölkənin rəqəmsallaşması, rəqəmsal dünyada müstəqil və dayanıqlı inkişafı üçün lazım olan texnoloji infrastrukturu əks etdirir. Bu səviyyəyə yeni texnologiyaların, telekommunikasiya infrastrukturlarının inkişafı və kibertəhlükəsizliklə bağlı indikatorlar daxildir. Bu səviyyə ölkələrin texnoloji infrastrukturunu inkişaf etdirmək, yerli bazarı gücləndirmək və strateji müttəfiqlik qurmaqla digər ölkələrdən asılılığı minimuma endirməyi hədəfləyir. İkinci səviyyə, idarəetmə səviyyəsi bir region üzərində suverenliyin təmin edilməsi üçün hüquqi və institutsional mexanizmləri nəzərə almalıdır. Buraya tənzimləyici tədbirlər, eləcə də, informasiya texnologiyalarının inkişafına yönəlmiş siyasətin

formalaşdırlması və strategiyaların hazırlanması daxildir. Bu səviyyə rəqəmsal ekosistemin idarə olunması, nəzarətdə saxlanması üçün institusional potensialı əks etdirir. Başqa sözlə, dövlət strukturlarının rəqəmsal ekosistemini idarə etmək, hüquqi tənzimləmə və nəzarət etmək gücü nəzərdə tutulur. Nəhayət, sosial suverenlik səviyyəsi vətəndaşların rəqəmsal texnologiyalardan necə istifadə etdikləri və onlara necə çıxış əldə etdiklərini əks etdirir. Bu göstəricilərə hər bir regionda internet istifadəçilərinin səviyyəsini göstərən rəqəmsal bacarıqlar və əlçatanlıq kimi amillər aid edilir. Qeyd olunan infrastruktur, idarəetmə və sosial səviyyələr bir-biri ilə bağlıdır və bu səviyyələr birləşərək ölkənin ümumarxitektur suverenlik ekosistemini formalaşdırır.

NƏTİCƏ

Rəqəmsal texnologiyaların sürətli inkişafı və kibertəhdidlərin artması şəraitində milli maraqların kiberməkanda qorunması məsələsi getdikcə daha da aktuallaşır. Kibersuverenlik milli təhlükəsizliyin əsas elementlərindən birinə çevrilir. Dövlətlər kiberməkanda rəqəmsal maraqlarını qorumaq üçün müxtəlif strategiyalar hazırlayırlar. Ədəbiyyat analizi göstərir ki, dövlətin kibersuverenliyinin səviyyələr üzrə strukturlaşdırılmasına dair fərqli yanaşmalar mövcuddur. Tədqiqat işində dövlət kibersuverenliyinə dair konseptual baxışlar, mövcud təhdidlər və risklər analiz olunmuşdur. Dövlətin kibersuverenliyinin arxitektur prinsipləri və funksional komponentləri araşdırılmışdır. Tədqiqat işində dövlətin kibersuverenliyinin təmin edilməsi üçün konseptual model təklif edilmişdir. Təklif olunan yanaşma infrastruktur, idarəetmə və sosial səviyyələrdən ibarətdir və bu səviyyələr birlikdə ölkənin kibersuverenlik ekosistemini formalaşdırır.

Hazırda kibersuverenlik konsepsiyasının reallaşdırılması mürəkkəb və çoxsahəli xarakter daşıyır və əksər ölkələr üçün onun tam şəkildə reallaşdırılması yaxın perspektivdə mümkün görünmür. Bu mənada rəqəmsal ekosistemin formalaşdırılması dövlətlər üçün aktual məsələlərdən biri olaraq qalmaqdadır. Kibertəhlükəsizlik baxımından bəzi ölkələrin telekommunikasiya avadanlıqlarının, rəqəmsal platformalarının istifadəsinə məhdudiyyət qoyulması ilkin addım hesab olunsa da bu həll yolu sayıla bilməz. Nəzərə almaq lazımdır ki, azad bazar mühitidə son dərəcə vacibdir və rəqəmsal platformalar üzərində ciddi nəzarət və onların fəaliyyətinə qoyulan məhdudiyyətlər də tamamilə düzgün yanaşma hesab olunmur. Bu sahədə uğur əldə etmək üçün ölkələr davamlı investisiya, innovasiya və hüquqi tənzimləmə ilə yerli texnologiya liderlərinin dəstəkləməsinə nail olmalıdırlar. Texnoloji monopoliyanı aradan qaldırmaq üçün tərəflərə bərabər imkanlar yaradılmalıdır. Bu isə beynəlxalq əməkdaşlıq və texnologiya transferinin daha ədalətli və davamlı əsaslar üzərində qurulmasına imkan verər.

ƏDƏBİYYAT

[1] A. Shoker, “Digital Sovereignty Strategies for Every Nation,” ACIG, vol. 1, no. 1, 2022. DOI: 10.5604/01.3001.0016.0943

[2] G. Falkner, S. Heidebrecht, A. Obendiek & T. Seidl, “Digital sovereignty - Rhetoric and reality,” Journal of European Public Policy, vol. 31(8), 2024, pp. 2099-2120, DOI: 10.1080/13501763.2024.2358984

[3] J. Leonard, D. Wu, K. Manson, “Taiwan Tensions Spark New Round of US War-Gaming on Risk to TSMC,” 2022. [Online]. Available: www.bloomberg.com/news/articles/2022-10-07/taiwan-tensionssparknew-round-of-us-war-gaming-on-risk-to-tsmc

[4]A. Follin, “Digital sovereignty in Europe: navigating the challenges of the digital era,” 2025. [Online]. Available: https://pppescp.com/2025/02/04/digital-sovereignty-in-europe-navigating-the-challenges-of-the-digital-era/

[5] J. Carver, “More bark than bite? European digital sovereignty discourse and changes to the European Union’s external relations policy,” Journal of European Public Policy, vol. 31(8), pp. 2250–2286. DOI: 10.1080/13501763.2023.2295523

[6] L. Leontyeva, M. Sukhareva, S. Volodenkov, and A. Voronov, “Digital sovereignty of a modern state in the context of technological transformations: Content and features,” Polylogos, vol. 5, no. 1, 2021. doi: 10.18254/S258770110014073-2

[7] J. Phole and T. Thiel, “Digital sovereignty,” Internet Policy Review, vol. 9, no. 4, 2020. DOI: 10.14763/2020.4.1532

[8] V. A. Nikonov, A. S. Voronov, V. A. Sazhina, S. V. Volodenkov, and M. V. Rybakova, “Tsifrovoy suverenitet sovremennogo gosudarstva: soderzhanie i strukturnye komponenty (po materialam ekspertnogo issledovaniya),” Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya, no. 60, 2021. (in Russian)

[9] B. Jansen, N. Kadenko, D. Broeders, M. van Eeten, K. Borgolte, and T. Fiebig, “Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions,” Government Information Quarterly, vol. 40, no. 4, 2023. DOI: 10.1016/j.giq.2023.101862.

[10] S. Galij, G. Pawlak, and S. Grzyb, “Modeling data sovereignty in public cloud – A comparison of existing solutions,” Applied Sciences, vol. 14, no. 23, 2024. DOI: 10.3390/app142310803

[11] “The EU’s digital challenges,” 2023. [Online]. Available: www.europarl.europa.eu/EPRS/TD_EUDigitalChallenges.pdf

[12] European Parliament, “Digital sovereignty for Europe: Towards a more resilient EU,” 2020. [Online]. Available: www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[14] M. del P. Rodríguez Pita, J. E. Pérez Martínez, and A. Urueña López, “From concept to method: A framework for measuring digital sovereignty,” in 33rd European Conference of the International Telecommunications Society (ITS): Digital Innovation and Transformation in Uncertain Times, Edinburgh, UK, Jun. 29–Jul. 1, 2025.

[15] L. Moerel and P. Timmers, “Reflections on digital sovereignty,” Rochester, Jan. 1, 2022. [Online]. Available: https://papers.ssrn.com/abstract=3772777

[16] European Commission, “Ethics guidelines for trustworthy AI,” Shaping Europe’s digital future, Apr. 8, 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[17] A. Obendiek, “Take back control? Digital sovereignty and a vision for Europe,” Jacques Delors Centre, Policy Paper, 2021.

[18] Council on Foreign Relations, Tracking state-sponsored cyberattacks around the world. [Online]. Available: www.cfr.org/cyber-operations

[19] Cybersecurity and Infrastructure Security Agency, CISA Strategic Plan 2023–2025, 2022. [Online]. Available:

www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf

[20] L. Floridi, "The fight for digital sovereignty: What it is, and why it matters, especially for the EU," Philosophy & Technology, vol. 33, no. 3, pp. 369–378, 2020. DOI: 10.1007/s13347-020-00423-6

[21] A. Braud, G. Fromentoux, B. Radier, and O. Le Grand, "The road to European digital sovereignty with Gaia-X and IDSA," IEEE Network, vol. 35, no. 2, pp. 4–5, 2021. DOI: 10.1109/MNET.2021.9387709

[22] T. Madiega, Digital sovereignty for Europe, European Parliamentary Research Service, European Parliament, 2020. [Online]. Available: www.europarl.europa.eu/RegData/etudes/-BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[15] P. Von Brockdorff, *Digital sovereignty: A crucial pillar for EU's digitalisation and growth*, European Economic and Social Committee, 2022. [Online]. Available: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-sovereignty-crucial-pillar-eus-digitalisation-and-growth

[16] A. Chander and H. Sun, *Sovereignty 2.0*, in *Data Sovereignty: From the Digital Silk Road to the Return of the State*, New York: Oxford Academic, 2023. DOI: 10.1093/oso/9780197582794.003.0001

[17] V. Shen and J. Kessler, *Competing values will shape US-China AI race*, 2024. [Online]. Available: https://www.thirdway.org/report/competing-values-will-shape-us-china-ai-race

[18] W. Cong, "The spatial expansion of China's digital sovereignty: Extraterritoriality and geopolitics," *SSRN Electronic Journal*, 2021. DOI: 10.2139/ssrn.4019797

[19] V. Carchidi and M. Soliman, *The role of the Middle East in the US-China race to AI supremacy*, 2024. [Online]. Available: https://www.mei.edu/sites/default/files/The%20Role%20of%20the%20Middle%20East%20in%20the%20Race%20to%20AI%20Supremacy.pdf

[20] "Tsifrovoy suverenitet: kak gosudarstva zashchishchayut svoi interesy v seti." [Online]. Available: https://www.it-world.ru/cionews/ogwlc57c1lw0k80g40kkw0wgwcckwwk.html (in Russian)

[21] L. Khasanova and K. Tai, "Shades of authoritarian digital sovereignty: Divergences in Russian and Chinese data localisation regimes," *Journal of Cyber Policy*, vol. 9, no. 1, pp. 70–94, 2024. DOI: 10.1080/23738871.2024.2413938

[22] M. Jiang, "Models of state digital sovereignty from the Global South: Diverging experiences from China, India and South Africa," *Policy & Internet*, Dec. 15, 2024. DOI: 10.2139/ssrn.5263970

[23] M. Kaloudis, "From quality to quantity: How can digital sovereignty be parsed into measurable," *European Journal of Business Science and Technology*, vol. 8, no. 2, pp. 172–189, 2022. DOI: 10.11118/ejobsat.2022.011

[24] G. León, *Autonomía estratégica abierta digital de la UE: Retos geopolíticos para la UE en un escenario convulso*, Fundación Alternativas, 2023. [Online]. Available: https://fundacionalternativas.org/wp-content/uploads/2023/10/-AUTONOMIA_ESTRATEGICA_DIGITAL_UE-1.pdf

Unified Architectural Principles and Functional Components of Government Cyber Sovereignty: Problems and Conceptual Approaches

Farhad Yusifov

Institute of Information Technology, Baku, Azerbaijan

Abstract— Digital transformati ons in public administration,along with the adoption of artificial intelligence technologies, introduce new challenges, and risks in ensuring government cyber sovereignty. This study examines the architectural principles ofgovernment cyber sovereignty and analyzes existing models proposed in the literature. Previous research demonstrates diverse approaches to structuring government cyber sovereignty across multiple levels. These approaches primarily encompass components such as technological infrastructure, data governance, and geopolitical considerations. This study proposes a conceptual model for ensuring government cyber sovereignty. The proposed framework consists of technological, governance, and social levels, which collectively form the cyber sovereignty ecosystem of a country.

Keywords— cyber sovereignty; public administration; government cyber sovereignty; digital technologies; artificial intelligence.