

Azərbaycan Rəqəmsal Suverenlik İndeksi: Analitik və Metodoloji Yanaşma

Lalə Kərimova

Azərbaycan Respublikası Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi, Bakı, Azərbaycan
lala.karimova@mincom.gov.az

Xülasə— Bu məqalə rəqəmsal suverenlik anlayışının ölçüləbilən və idarəolunan alətə çevrilməsi məqsədilə yanaşmanı təhlil edir. Araşdırmada beynəlxalq təcrübədə mövcud olan konseptual və indikator-əsaslı modellər müqayisə olunur, onların üstün və məhdud cəhətləri müəyyənləşdirilir. Məqalə Azərbaycan Rəqəmsal Suverenlik İndeksinin (AzRSİ) metodologiyasını təqdim edir. Təklif olunan model rəqəmsal infrastruktur, məlumat, texnologiya, tənzimləmə, insan kapitalı və kibərdayanıqlılıq aspektlərini inteqrə olunmuş şəkildə qiymətləndirməyə imkan yaradır.

Açar sözlər— rəqəmsal suverenlik; rəqəmsal suverenlik matrisi; rəqəmsal suverenlik indeksi; kibərdayanıqlılıq.

I. GİRİŞ

Rəqəmsal suverenlik anlayışı dövlətlərin, ictimai institutların və fərdi vətəndaşların öz rəqəmsal infrastrukturunu, məlumatları, standartları və qərarvermə hüququ üzərində nəzarət və müstəqilliyini təmin etmə bacarığını ifadə edir. Bu konsepsiya ənənəvi suverenlik anlayışının, yəni fiziki sərhədlər çərçivəsindən fərqli olaraq informasiya və texnologiya müstəvisində özünü idarəetmə hüququnun rəqəmsal dünyaya uyğunlaşdırılmış versiyasıdır [1-3].

Rəqəmsal suverenlik məhz rəqəmsal iqtisadiyyatın, kritik infrastrukturun və məlumatın strateji əhəmiyyət qazandığı bir dövrdə aktualdır. COVID-19 pandemiyası, qlobal təchizat zəncirlərindəki gərginliklər, kibercinayətkarlıq və informasiya müharibələri kimi faktorlar ölkələri öz rəqəmsal sistemlərini xarici təsirlərdən qorumağa yönəldir ki, bu da rəqəmsal suverenlik anlayışının mühüm ictimai və siyasi məqsəd olmasını təmin edir.

Dünyanın əksər ölkələrinin texnologiya və rəqəmsal platformalar üzrə əsasən ABŞ və Çin mənşəli şirkətlərdən asılılığı, xüsusilə süni intellekt, bulud xidmətləri, yüksək performanslı hesablama və 5G kimi strateji texnologiya sahələrində bu ölkələrin lider mövqeyi, qlobal miqyasda həm informasiya, həm də strateji asılılıq səviyyəsinin artmasına səbəb olur. Avropa İttifaqı, məsələn, GDPR, Digital Markets Act və digər normativ aktlar vasitəsilə rəqəmsal hüquq və məxfilik prinsiplərini gücləndirməyə çalışır ki, bu da rəqəmsal suverenliyin hüquqi təməlini formalaşdırır. Rəqəmsal suverenlik çərçivəsi qapalı iqtisadi modellərin tətbiqini və “tam müstəqillik” deyil, müstəqillik və beynəlxalq inteqrasiya arasında balans tapmaq, iqtisadi inkişaf və milli təhlükəsizlik arasında əlaqə üçün bir vasitə kimi nəzərdə tutulur.

Bu yanaşmalar göstərir ki, rəqəmsal suverenlik artıq yalnız normativ və ya siyasi məqsəd deyil, ölçüləbilən, idarə olunan və mərhələli şəkildə inkişaf etdirilən bir siyasət sahəsinə

çevrilməlidir. Məhz bu ehtiyac ölkələrin mövcud asılılıqlarını və texnoloji potensiallarını, eləcə də risk və imkanlarını sistemli şəkildə təhlil edə bilən analitik alətlərin tətbiqini zəruri edir. Bu baxımdan, konseptual prinsiplərin praktik qərarvermə mexanizmlərinə çevrilməsi üçün strukturlaşdırılmış və müqayisə oluna bilən bir qiymətləndirmə modelinə keçid obyektiv ehtiyac kimi meydana çıxır.

Açıq mənbələrdə “Rəqəmsal Suverenlik Matrisi” (RSM) və ya oxşar strukturlar, müxtəlif çərçivələr, indikatorlar və meyarlar şəklində əks olunan regional icmallar, akademik məqalələr, beynəlxalq təşəbbüslər və s. kimi resurslar mövcuddur. Ölkələrin və regionların rəqəmsal sahədə imkanlarını hərtərəfli qiymətləndirmək üçün praktik çərçivə olan RSM konsepsiyası vasitəsilə dövlətlər məlumat və texnoloji infrastrukturunu öz nəzarəti altında saxlaya, kibertəhlükəsizlik risklərini daha yaxşı idarə edə, strateji texnoloji investisiyaları və koordinasiyanı təyin edə, beynəlxalq rəqabətdə öz mövqelərini gücləndirə bilərlər. Ümumiyyətlə, bu və digər yanaşmalar çoxölçülü qiymətləndirmə sistemlərində, fərqli modellərdə, tədqiqat təşəbbüslərində, müxtəlif sahələr üzrə suverenlik meyarlarını əhatə edən analitik platformalarda öz əksini tapır. Məsələn, “Digital Sovereignty Assessment Matrix - Sustainable Digital Infrastructure Alliance (SDIA)” [4], WIK-Consult tərəfindən hazırlanmış “Digital Sovereignty Report” [5], “European Digital Infrastructure and Data Sovereignty” [6], “Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models” [7], “Internet Society - Digital Sovereignty Toolkit” [8], “Digital Sovereignty Observatory - Interdisciplinary Research Platform” [9], Nextcloud şirkətinin Rəqəmsal Suverenlik İndeksi, “Cloud Sovereignty Framework” [10] və s.

Beləliklə, məqalənin əsas məqsədi rəqəmsal suverenlik anlayışının mövcud nəzəri və praktik yanaşmalarını sistemləşdirmək, onların müqayisəli təhlilini aparmaq və ölçüləbilən analitik çərçivələrin əhəmiyyətini əsaslandırmaqdır. Bu kontekstdə tədqiqat rəqəmsal asılılıqların idarəolunması və strateji qərarvermə üçün tətbiq oluna bilən metodoloji yanaşmaların formalaşdırılmasına töhfə verməyi hədəfləyir.

II. RƏQƏMSAL SUVERENLİYİN ANALİTİK QIYMƏTLƏNDİRMƏ ÇƏRÇİVƏLƏRİ

A. “Digital Sovereignty Report”

WIK-Consult hesabatı rəqəmsal suverenlik anlayışını sistemli şəkildə təhlil edərək, xüsusilə Avropada rəqəmsal suverenliyin vəziyyətini qiymətləndirir. Hesabatın əsas məqsədi Avropa İttifaqının və üzv dövlətlərinin rəqəmsal

müstəqillik səylərini müqayisəli baza üzərində göstərmək, mövcud çətinlikləri müəyyənləşdirmək və ümumi meyilləri təsvir etməkdir [5].

Hesabatda RSM termini geniş şəkildə izah olunmasa da, rəqəmsal suverenlik elementləri və göstəricilər bir matris yanaşması kimi strukturlaşdırılır. Bu struktur əsasən aşağıdakı üç əsas göstərici üzərində qurulur:

- **Məxfilik və məlumat suverenliyi (Privacy/Data Sovereignty):** Bu göstərici məlumat üzərində nəzarət hüququnu əhatə edir, yəni şəxsə və dövlətə məxsus məlumatların müstəqil qaydada idarə olunması, qorunması və hüquqi müstəvidə nəzarətinin təmin edilməsini nəzərdə tutur;
- **Kibertəhlükəsizlik suverenliyi (Cybersecurity Sovereignty):** Kritik informasiya infrastrukturalarının etibarlı qorunmasının təmin edilməsi, xarici vətəndaşlardan və ya şirkətlərdən həddindən artıq asılılığın azaldılması bu göstəricinin ideya mərkəzindədir;
- **Strateji və geosiyasi suverenlik (Strategic/Geopolitical Sovereignty):** Rəqəmsal texnologiyalar sahəsində iqtisadi, siyasi və strateji qərarvermə azadlığı bu göstərici ilə qiymətləndirilir. Burada yalnız texnologiyaya sahib olmaq deyil, həm də beynəlxalq arenada rəqabət apara biləcək strateji imkanların olması nəzərdə tutulur.

Bu üç əsas göstəricinin kombinasiyası faktiki olaraq RSM funksiyasını yerinə yetirir və ölkələrin rəqəmsal mühitdə strateji müstəqillik səviyyəsini, dayanıqlılığını və idarəetmə potensialını müqayisəli şəkildə dəyərləndirməyə şərait yaradır.

B. “Digital Sovereignty Assessment Matrix”

Hazırda rəsmi RSM modeli kimi açıq şəkildə istifadə olunan nümunələrdən biri Sustainable Digital Infrastructure Alliance e.V. (SDIA) [11] tərəfindən hazırlanmış “Digital Sovereignty Assessment Matrix (DSAM)”dır [12]. 2019-cu ildə təsis edilmiş və Almaniyanın Hamburq şəhərində yerləşən SDIA davamlı rəqəmsal iqtisadiyyata keçidi sürətləndirmək məqsədilə fəaliyyət göstərən 65-dən çox üzv və tərəfdaşı birləşdirən qeyri-kommersiya şəbəkəsidir. SDIA həm rəqəmsal infrastrukturaların strateji qiymətləndirilməsi, həm də regionların rəqəmsal müstəqilliyi ilə bağlı çərçivələr üzərində işləyir, bu da birbaşa rəqəmsal suverenlik matrislərinin hazırlanması üçün faydalı metodoloji əsas yaradır. Bu matris konkret göstəricilər üzrə dövlətin və ya regionun rəqəmsal suverenliyini ölçmək və qiymətləndirmək üçün istifadə edilir.

DSAM çoxölçülü analitik çərçivə kimi formalaşdırılaraq, rəqəmsal suverenliyin əsas komponentlərini strukturlaşdırılmış indikatorlar sistemi vasitəsilə qiymətləndirir. Matris adətən məlumatların idarə olunması, rəqəmsal infrastruktur, platforma asılılığı və texnoloji nəzarət kimi əsas sahələr üzrə qurulur. Hər bir sahə konkret göstəricilər və altgöstəricilər vasitəsilə ölçülür ki, bu da rəqəmsal mühitdə xarici asılılıq səviyyəsini empirik şəkildə müəyyən etməyə imkan verir. Qiymətləndirmə prosesi yalnız texniki imkanlarla məhdudlaşmır, eyni zamanda hüquqi və geosiyasi amilləri, idarəetmə imkanlarını da nəzərə alır. Matrisin iş prinsipi müxtəlif göstəricilər üzrə əldə olunan

nəticələrin inteqrasiyasına əsaslanaraq ümumi rəqəmsal suverenlik profilinin formalaşdırılmasını nəzərdə tutur. Bu yanaşma ölkələr və regionlar arasında müqayisəli təhlil aparmağa şərait yaradır. Eyni zamanda, matris boşluqlar olan sahələrin və strateji risklərin müəyyən edilməsinə imkan verərək siyasət formalaşdırılması üçün analitik əsas rolunu oynayır. Nəticə etibarilə, DSAM rəqəmsal müstəqilliyin mövcud vəziyyətini ölçməklə yanaşı, onun gücləndirilməsi üçün prioritet istiqamətləri müəyyən edən metodoloji alət kimi çıxış edir. SDIA və WIK-Consult yanaşmalarının müqayisəsi Cədvəl 1-də təqdim olunur.

CƏDVƏL 1. SDIA VƏ WIK-CONSULT YANAŞMALARININ MÜQAYISƏLİ TƏHLİLİ

Müqayisəmə yarı	SDIA - Digital Sovereignty Assessment Matrix	WIK-Consult yanaşması
Əsas məqsəd	Dövlət və regionların rəqəmsal suverenlik səviyyəsini praktik və ölçülə bilən indikatorlar vasitəsilə qiymətləndirmək	Rəqəmsal suverenliyi struktur, bazar və tənzimləmə müstəvisində konseptual və siyasət yönümlü şəkildə təhlil etmək
Metodoloji yanaşma	İndikator-əsaslı, çoxölçülü analitik matris	Konseptual çərçivə, müqayisəli siyasət və analiz
Ölçmə səviyyəsi	Təbiiq yönümlü (praktik qiymətləndirmə aləti)	Makro-səviyyəli və strateji
Əsas fokus sahələri	Məlumat, platforma, texnologiya və infrastruktur asılılığı	İnfrastruktur ekosistemi, bazar strukturları, tənzimləyici mühit
Asılılıq anlayışı	Xarici texnologiya və platformalardan asılılığın birbaşa ölçülməsi	Asılılığın iqtisadi və strateji nəticələrinin təhlili
Risklərin qiymətləndirilməsi	Geosiyasi, texnoloji və əməliyyat risklərinin indikatorlar üzrə müəyyən edilməsi	Sistemli risklər və siyasət boşluqları üzərindən keyfiyyət analizi
İstifadəçi hədəfi	Qərarvericilər, regional idarəetmə orqanları, layihə planlaşdırıcıları	Siyasət formalaşdırıcı qurumlar, tədqiqatçılar, strateji analitiklər
Əsas nəticə	Rəqəmsal suverenlik üzrə mövcud vəziyyətin ölçülməsi və prioritet sahələrin müəyyənəndirilməsi	Rəqəmsal suverenlik siyasətlərinin formalaşdırılması üçün analitik əsas

C. Rəqəmsal Suverenlik İndeksi

Rəqəmsal Suverenlik İndeksi (Digital Sovereignty Index – DSI) [13] hər ölkənin özü tərəfindən yerləşdirilmiş (“self-hosted”) infrastrukturunun təhlili nəticəsində ölkələrin müqayisəli mənzərəsini təqdim edir. Bu indeks hər ölkənin öz rəqəmsal resurslarına, infrastrukturuna və məlumatlarına nə dərəcədə nəzarət etdiyini və xarici texnoloji resurslardan asılılığını təyin edir, faktiki olaraq yerli alətlərin real istifadəsini ölçməyə cəhd edir. DSI balı, əhalinin hər 100 min nəfərinə düşən “self-hosted” alətlərinin quraşdırılma (“deployment”) sayının digər ölkələrlə müqayisədə nisbi göstəricisini əks etdirir.

DSI – Almaniyanın “open-source” proqram təminatı şirkəti Nextcloud tərəfindən ilk dəfə 2025-ci ildə hazırlanmış indeksdir və təxminən 50-dən çox ölkənin (əsasən Yaxın-Şərq,

Avropa, Şimali Amerika və s.) rəqəmsal suverenliyi səviyyəsini ölçür.

Şəkil 1-də DSI göstəricilərinin dünya xəritəsi üzərində vizual təsviri təqdim olunur. Xəritədə ölkələr rəqəmsal suverenlik səviyyəsinə uyğun olaraq müxtəlif rəng çalarları ilə işarələnmişdir. Bu şkala ölkələr üzrə DSI balının müqayisəli şəkildə qiymətləndirilməsinə imkan yaradır: daha aşağı göstəricilər zəif rəqəmsal suverenlik səviyyəsini, daha yüksək göstəricilər isə yerli rəqəmsal infrastrukturdan və “self-hosted” həllərdən daha geniş istifadəni ifadə edir.



Şəkil 1. Rəqəmsal suverenlik xəritəsi

Nümunə olaraq, Türkiyə üzrə təqdim edilən göstəricilər ölkədə 73 245 serverin qeydə alındığını, əhalinin isə təxminən 84.6 milyon nəfər olduğunu göstərir. Bu göstəricilər əsasında Türkiyənin DSI balı 2.26 kimi qiymətləndirilmişdir. Bu nəticə əhali sayına nisbətə “self-hosted” alətlərin tətbiq səviyyəsinin məhdud olduğunu və rəqəmsal suverenlik potensialının daha da inkişaf etdirilməsinə ehtiyac olduğunu göstərir. Ümumilikdə, DSI nəticələri rəqəmsal suverenliyin yalnız hüquqi və siyasi iradə ilə deyil, həm də real infrastruktur imkanları, yerli texnoloji həllərin tətbiqi və rəqəmsal xidmətlərin daxili ekosistem daxilində yerləşdirilməsi ilə ölçülməli olduğunu nümayiş etdirir.

“Self-hosted” infrastruktur dedikdə, proqram və rəqəmsal xidmətlərin xarici korporasiyalar, provayderlər (məsələn, Google, Microsoft, Amazon və s.) tərəfindən deyil, birbaşa istifadəçi, təşkilat və ya qurumun öz nəzarətində olan serverlər üzərində qurulması və idarə olunması başa düşülür. Məlumatlar və sistemlər təşkilatın öz fiziki serverlərində və ya nəzarətində olan virtual serverlərdə saxlanılır, mərkəzləşdirilməmiş xidmətlərin fəaliyyəti xarici korporasiyaların infrastrukturundan asılı olmur, məlumatların harada saxlanıldığı, kim tərəfindən və necə istifadə edildiyi tam şəkildə sahibin nəzarətində olur, texnoloji müstəqillik təmin olunur, yəni proqram təminatının konfiqurasiyası, yenilənməsi və təhlükəsizlik siyasəti yerli təşkilat və ya qurum tərəfindən müəyyən edilir. Nəticə etibarlı ilə “self-hosted” infrastruktur rəqəmsal xidmətlərin istifadəsində idarəetmə, məlumat və texnoloji nəzarətin birbaşa istifadəçidə (və ya qurumun özündə) olduğu modeli nəzərdə tutur və bu səbəbdən rəqəmsal suverenliyin əsas komponentlərindən biri hesab olunur.

DSI-də fayl paylaşımı, video konfrans, elektron poçt, layihə idarəetməsi və s. platformaları əhatə edən ən aktual 50 “self-hosted” aləti qiymətləndirilir. Daha sonra onların real istifadə səviyyəsi - ölkələr üzrə internet üzərindən mövcudluğu və yerləşdiyi ölkə texniki üsullarla müəyyən edilə bilən aktiv server qurğularının (server nüsxələrinin) sayı hesablanır (2025-ci ildə araşdırma təxminən 7,2 milyon server üzərində aparılıb). Nəticə ölkədə həmin texnologiyaların 100K nəfər əhaliyə

düşən istifadə sayı 0-100 arası bal şəklində təqdim edilir və bu, ölkənin indeks göstəricisi kimi təyin olunur.

Ümumiyyətlə, indeks ölkələrin öz IT infrastrukturunun, onun üzərində nəzarətin və yerli həllərin tətbiq səviyyəsini ölçür. Buna görə də DSI rəqəmsal suverenlik matrisi üçün real ölçü meyarı baxımından faydalı ola və dövlətlərin hansı sahələrdə daha çox xarici asılılığa malik olduğunu göstərə bilər.

D. Çinin rəqəmsal suverenlik modeli

Çin Xalq Respublikasının radikal rəqəmsal suverenlik modeli dövlətin milli informasiya məkanına tam hüquqi nəzarət tətbiq etməsinə əsaslanan yanaşmadır. Bu model çərçivəsində rəqəmsal infrastruktur, məlumat axınları, platformalar və onlayn kontent dövlət tərəfindən tənzimlənir, məlumatların ərazi daxilində saxlanması və transsərhəd məlumat ötürülməsinin məhdudlaşdırılması hüquqi mexanizmlərlə təmin edilir. Modelin əsas məqsədi milli təhlükəsizliyin, ictimai sabitliyin və texnoloji suverenliyin qorunmasıdır. Model dövlətə kibertəhlükəsizlik risklərini minimuma endirmək, milli texnologiya sektorunu qorumaq və strateji məlumatlar üzərində nəzarəti gücləndirmək imkanı yaradır. Eyni zamanda yerli rəqəmsal platformaların inkişafını və daxili bazarın konsolidasiyasını stimullaşdırır. Lakin bu radikal yanaşma, sərt dövlət nəzarəti informasiya azadlığını və rəqəmsal hüquqları məhdudlaşdırır, innovasiya və beynəlxalq elmi-texnoloji əməkdaşlıq üçün maneələr yarada bilər. Bundan əlavə, qlobal internet ekosistemi ilə inteqrasiyanın zəifləməsi uzunmüddətli iqtisadi və texnoloji rəqəbat qabiliyyətinə mənfi təsir göstərə bilər [14-16].

Hazırkı mərhələdə böyük daxili bazar, güclü dövlət-özəl sektor sinerjisi və məqsədyönlü sənaye siyasəti yerli innovasiya ekosisteminin formalaşmasını sürətləndirir. Süni intellekt, fintech, 5G və e-ticarət sahələrində Çin qapalı model daxilində belə qlobal liderliyə yaxın mövqelər əldə edib. Lakin bu dinamika struktur üstünlüklərə (əhali ölçüsü, kapital, dövlət koordinasiyası) əsaslanır və uzunmüddətli perspektivdə bilik mübadiləsinin məhdudlaşması, standartların qlobal formalaşmasında iştirakın azalması və texnoloji “paralelləşmə” riski yarada bilər. Yəni Çin hazırda böyük irəliləmə əldə etsə də, bu modelin davamlılığı qlobal texnoloji arxitekturanın formalaşacağından asılı olacaq.

Çin bu konsepsiyayı beynəlxalq tədqiqatlarda “cyber sovereignty” olaraq xarakterizə edən dövlət-mərkəzli internet idarəçiliyi modelinə aid edir. Bu modeldə hər bir dövlətin öz internet məkanını öz qanunları və siyasətləri çərçivəsində tənzimləmək hüququ və hakimiyyətin xarici təsirlərdən qorunmasının zəruriliyi vurğulanır [17]. Akademik tədqiqatlarda Çinin kibersuverenlik konsepti “milli suverenliyin informasiya və kommunikasiya texnologiyası platformalarına tətbiqi” kimi təsvir edilir və bu yanaşma Çin hökumətinin şəbəkə təhlükəsizliyi, məlumat axını və onlayn kontent üzərində nəzarət mexanizmlərini ehtiva edir [18]. Çinin Kibertəhlükəsizlik Qanunu da rəsmi olaraq “cyberspace sovereignty” prinsipini hüquqi baza səviyyəsində tanıyır. Bu qanuna görə Çin dövləti şəbəkə təhlükəsizliyi və rəqəmsal məkanı milli suverenlik kontekstində qorumaq məqsədilə qaydalar müəyyənləşdirir [19].

Beləliklə, Çin modeli xüsusilə kibertəhlükəsizlik, kritik infrastrukturaların qorunması, məlumat (“data”) lokalizasiyası və milli platformaların dəstəklənməsi baxımından funksional alətlər təqdim edir. Dövlətin koordinasiyaedici rolu zəif olan və ya xarici texnologiyalardan yüksək asılılığı olan ölkələr üçün bu elementlər rəqəmsal dayanıqlılığı artırır. Lakin modelin birbaşa tətbiqi informasiya azadlığı, innovasiya ekosistemi və beynəlxalq inteqrasiya baxımından risklər yaradır. Buna görə açıq internet, qlobal standartlar və bazar rəqabəti baxımından səmərəli praktik yanaşma modeli hesab edilə bilməz.

E. Rəqəmsal Suverenlik Matrisi - RSM

Araşdırmalar göstərir ki, RSM-ə dövlətin xarici rəqəmsal platformalardan, texnologiyalardan və məlumat infrastrukturundan asılılıq səviyyəsini sistemli şəkildə ölçən analitik qiymətləndirmə aləti kimi baxa bilərik. Adətən bu matris Cədvəl 2-dəki aşağıdakı blokları ehtiva edir:

CƏDVƏL 2. RSM BLOKLARI ÜZRƏ ƏSAS GÖSTƏRİCİLƏR VƏ MEYARLAR

Bloklar	Əsas göstəricilər	Qiymətləndirmə meyarları
Məlumat suverenliyi	Məlumatların saxlanma yeri və hüquqi yurisdiksiya	Məlumatların ölkə daxilində və ya xaricdə saxlanılması; xarici hüquqi rejimlərə (məsələn, extraterritorial qanunlar) tabeçilik
	Məlumatlara çıxış və emal subyektləri	Dövlət qurumları, yerli və xarici özəl şirkətlər, üçüncü tərəf provayderlər
	Məlumatların mühafizəsi və məxfilik mexanizmləri	Şifrələmə standartları, məlumat təhlükəsizliyi protokolları, milli “data protection” rejimi
Platforma suverenliyi	Rəqəmsal platformaların mənşəyi və mülkiyyət strukturu	Yerli / regional / qlobal (xarici) platformalardan istifadə səviyyəsi
	Platformaların iqtisadi və sosial təsir dairəsi	İstifadəçi payı, bazar konsentrasiyası, dövlət və ictimai kommunikasiya üçün əhəmiyyəti
	Tənzimləmə və nəzarət imkanları	Milli qanunvericiliklə uyğunluq, platforma üzərində dövlət nəzarət mexanizmləri
Texnoloji suverenlik	Əsas texnologiyaların mənşəyi	Əməliyyat sistemləri, server infrastrukturunu, bulud texnologiyaları
	Süni intellekt və alqoritmik asılılıq	Süni intellekt modellərinin yerli və ya xarici mənşəli olması, təlim “data”-sına nəzarət
	Kriptoqrafiya və təhlükəsizlik texnologiyaları	Şifrələmə alqoritmləri, milli kripto-standartların mövcudluğu
Risk və dayanıqlılıq	Geosiyasi və siyasi risklər	Sanksiya riski, siyasi təzyiqlər, texnoloji embarqo ehtimalı
	İnformasiya təhlükəsizliyi riskləri	Dezinformasiya, alqoritmik manipulyasiya, platforma senzurası
	Sistem dayanıqlılığı və davamlılıq	Kiberhücumlara dayanıqlılıq, kritik infrastrukturun qorunması

Bu cədvəl RSM çərçivəsində dövlətin rəqəmsal ekosistem üzərində nəzarət, müstəqillik və dayanıqlılıq səviyyəsini ölçmək üçün əsas analitik ölçüləri və indikatorları sistemləşdirir. RSM məlumat, platforma və texnologiya sahələrində xarici asılılıq dərəcəsini, eləcə də bu asılılıqlardan irəli gələn strateji və təhlükəsizlik risklərini kompleks şəkildə qiymətləndirməyə imkan verir.

III. RƏQƏMSAL SUVERENLİYİN İNTEQRƏ EDİLMİŞ QIYMƏTLƏNDİRMƏ MODELİ ÜÇÜN YANAŞMA

Son illərdə rəqəmsal texnologiyaların iqtisadiyyatın, dövlət idarəçiliyinin və ictimai kommunikasiya mühitinin əsas komponentinə çevrilməsi rəqəmsal suverenlik məsələsini Azərbaycan üçün də strateji əhəmiyyətli gündəm mövzusunə çevirmişdir. Dövlətin xarici rəqəmsal platformalar, texnologiyalar və məlumat infrastrukturundan asılılıq səviyyəsinin ölçülməsi və idarə olunması məqsədilə RSM analitik çərçivə kimi tətbiq oluna bilər. Təqdim olunan nümunə - RSM modeli SDIA-nın indikator-əsaslı qiymətləndirmə yanaşması ilə WIK-Consult-ın siyasət yönümlü analiz çərçivəsinin sintezinə əsaslanır.

Tətbiq üçün təklif olunan RSM altı əsas analitik blok üzərində qurulur: rəqəmsal infrastruktur suverenliyi, məlumat suverenliyi, texnoloji suverenlik, tənzimləyici suverenlik, kadrlar/innovasiya və dayanıqlılıq. Hər bir blok üzrə ölçmə kəmiyyət (asılılıq səviyyəsi) və ya keyfiyyət (idarəetmə və tənzimləmə imkanları) meyarlarını əhatə edə bilər. Bu yanaşma rəqəmsal suverenliyi yalnız texniki məsələ kimi deyil, eyni zamanda idarəetmə və geosiyasi fenomen kimi qiymətləndirməyə imkan verir. Azərbaycan üzrə rəqəmsal suverenliyin analitik bloklar əsasında ilkin vəziyyəti Cədvəl 3-də təqdim olunur.

CƏDVƏL 3. ÖLKƏ ÜZRƏ RƏQƏMSAL SUVERENLİK VƏZİYYƏTİNİN İLKİN QIYMƏTLƏNDİRİLMƏSİ

Analitik blok	Əsas göstəricilər	Azərbaycan üzrə müşahidə edilən vəziyyət
1. Rəqəmsal infrastruktur suverenliyi	<i>Milli data-mərkəzlərin payı</i>	Dövlətə məxsus və lokal data-mərkəzlər mövcuddur, lakin ümumi trafik və kommersiya məlumatlarının əhəmiyyətli hissəsi xarici mərkəzlərdə saxlanılır. Azərbaycanda Superkompüter Mərkəzi qurulub [20].
	Telekom şəbəkələrinə nəzarət (fiber, 4G/5G)	Əsas telekom infrastrukturunu milli operatorların nəzarətindədir; avadanlıq səviyyəsində idxaldan asılılıq qalır
	Milli bulud platformaları	Dövlət sektoru üçün məhdud həcmdə mövcuddur, özəl sektor əsasən xarici buludlardan istifadə edir
2. Məlumat suverenliyi	Məlumatların idarə edilməsi	Bəzi hüquqi mexanizmlər mövcuddur. Dövlət məlumatlarının əhəmiyyətli hissəsi ölkə daxilində saxlanılır, lakin kommersiya və sosial məlumatlar üçün tətbiq selektivdir. Xarici bulud və platforma provayderlərinin üstün mövqeyi mövcuddur.

	Milli reyestrələr və e-hökumət platformaları	Güclü inkişaf edib (Mygov, ASAN)
	Kritik datanın daxilədə saxlanması imkanı	Dövlət məlumatları üzrə yüksək, özəl sektor üzrə orta səviyyə
3. Texnoloji suverenlik	İdxal proqram təminatı və “hardware” payı	OS, server, şəbəkə avadanlıqları əsasən idxal mənşəlidir.
	Yerli OS, çiplər, AI modelləri	Məhdud və erkən mərhələdə təşəbbüslər mövcuddur
	Big Tech-ə asılılıq	Bulud, AI və platforma xidmətlərində orta-yüksək asılılıq mövcuddur.
	Platforma müstəqilliyi	Əsas sosial media və ictimai kommunikasiya kanalları xarici (qeyri-regional) platformalara əsaslanır
4. Tənzimləyici suverenlik	Rəqəmsal qanunvericilik	Əsas hüquqi baza mövcuddur, lakin icra və texniki nəzarət mexanizmləri zəifdir
	Antimonopol və platforma tənzimlənməsi	Qismən mövcuddur, qlobal platformalar üzərində təsir məhduddur
	Transsərhəd “data” axınlarına nəzarət	Formal mexanizmlər var, faktiki nəzarət zəifdir
5. Kadrlar və innovasiya	IT mütəxəssislərinin sayı	Artan trend mövcuddur, lakin beyin axını riski qalır
	R&D və innovasiya ekosistemi	Dövlət təşviqləri var, özəl sektorun payı məhduddur
	Startaplar və patentlər	Erkən inkişaf mərhələsində, regional rəqabət hələ zəifdir
6. Dayanıqlılıq	Geosiyasi və sanksiya riskləri	Regional və qlobal proseslərdən potensial risk mövcuddur
	İnformasiya manipulyasiyası riski	Xarici platformalar üzərindən orta səviyyəli risk mövcuddur

RSM-ə bu yanaşma göstərir ki, Azərbaycanda rəqəmsal suverenlik əsasən platforma və texnoloji asılılıq istiqamətində zəif mövqedədir. Məlumatların hüquqi baxımdan qorunması üçün baza mövcud olsa da, faktiki “data” axınları üzərində nəzarət imkanları məhduddur. Bu vəziyyət ölkənin rəqəmsal ekosisteminə xarici texnoloji qərarlardan və geosiyasi dəyişikliklərdən asılı hala gətirir. WIK-Consult yanaşmasına uyğun olaraq bu asılılıq yalnız texniki deyil, eyni zamanda strateji və idarəetmə problemdir.

SDIA modelinin praktik indikatorları Azərbaycanda rəqəmsal asılılıq sahələrinin konkret şəkildə müəyyən edilməsinə imkan verdiyi halda, WIK-Consult yanaşması bu nəticələrin dövlət siyasəti səviyyəsində necə cavablandırılmalı olduğunu göstərir. RSM-in müntəzəm tətbiqi rəqəmsal infrastruktur investisiyalarının prioritetləşdirilməsi, yerli texnoloji ekosistemin gücləndirilməsi və tənzimləyici mexanizmlərin təkmilləşdirilməsi üçün əsas analitik alət rolunu oynaya bilər.

Beləliklə, RSM Azərbaycanda rəqəmsal müstəqilliyin mövcud vəziyyətini ölçmək, riskləri erkən mərhələdə müəyyən etmək və strateji qərarların əsaslandırılması üçün effektiv metodoloji çərçivə kimi istifadə oluna bilər. SDIA və WIK-

Consult yanaşmalarının sintezi isə həm ölçülə bilən nəticələr, həm də uzunmüddətli siyasət baxımından balanslaşdırılmış yanaşma təqdim edir.

SDIA və WIK-Consult yanaşmalarına Rəqəmsal Suverenlik İndeksi (Digital Sovereignty Index, DSI) metodologiyasının əlavə edilməsi rəqəmsal suverenliyin ölçülməsində konseptual-praktik boşluğu əhəmiyyətli dərəcədə azalda bilər. WIK-Consult yanaşması rəqəmsal suverenliyi struktur, bazar və tənzimləmə mühiti kontekstində makro-səviyyəli strateji problem kimi təhlil etdiyi halda, SDIA modeli bu anlayışı indikator-əsaslı və operasional qiymətləndirmə çərçivəsinə çevirir. DSI isə bu iki yanaşmanı empirik istifadə göstəriciləri ilə tamamlayaraq real vəziyyətin ölçülməsinə imkan yaradır. İntegr edilmiş modeldə WIK-Consult çərçivəsi suverenliyin niyə və hansı struktur səbəblərdən zəif və ya güclü olduğunu, SDIA matrisi harada və hansı sahələr üzrə asılılıq mövcud olduğunu, DSI isə bu asılılığın real istifadədə nə dərəcədə özünü göstərdiyini nümayiş etdirir. Nəticədə rəqəmsal suverenlik həm normativ-strateji, həm analitik-ölçmə, həm də empirik-istifadə səviyyəsində qiymətləndirilmiş olur.

DSI-nin əsas üstünlüyü rəqəmsal suverenliyi yalnız hüquqi və idarəçilik imkanları səviyyəsində deyil, yerli (“self-hosted”) rəqəmsal alətlərin faktiki istifadəsi əsasında ölçməsidir. Beləliklə, SDIA matrisində müəyyən edilən potensial və risklər DSI vasitəsilə real istifadə davranışları ilə yoxlanılır. Bu yanaşma “mövcud imkanlar” ilə “praktik tətbiq” arasında fərqin aşkarlanmasına şərait yaradır.

Bu sintez rəqəmsal suverenliyin “yalnız siyasət sənədi”, “yalnız indikator cədvəli” və ya “yalnız indeks” kimi məhdud çərçivələrdə qiymətləndirilməsinin qarşısını alır və çoxsəviyyəli analitik model formalaşdırır. Xüsusilə inkişaf etməkdə olan və orta ölçülü iqtisadiyyatlar üçün bu yanaşma strateji ambisiyalarla real texnoloji imkanlar arasındakı uyğunsuzluqları aşkar etməyə imkan verir.

Bu üç yanaşmanın birgə tətbiqi rəqəmsal suverenliyin yalnız qanunvericilik və dövlət proqramları səviyyəsində deyil, həm də yerli rəqəmsal alətlərin real istifadə intensivliyi baxımından qiymətləndirilməsinə imkan yaradır. Bu isə rəqəmsal strategiyaların effektivliyinin ölçülməsi və prioritetlərin daha dəqiq müəyyən edilməsi üçün etibarlı analitik baza yaradır.

IV. AZRSİ – AZƏRBAYCAN RƏQƏMSAL SUVERENLİK İNDEKSİ

RSM altı əsas analitik bloku əsasında Azərbaycan Rəqəmsal Suverenlik İndeksinin hesablanma metodologiyasını təqdim edirik. Yeni indeksin hazırlanmasına ehtiyac bir neçə fundamental səbəblərdən irəli gəlir.

- mövcud indekslər rəqəmsal inkişafı ölçsə də, rəqəmsal asılılıqları və suverenlik risklərini ayrıca kateqoriya kimi qiymətləndirmir. Halbuki rəqəmsal infrastrukturun xarici texnologiyalardan asılılığı, “data” axınlarının nəzarətsizliyi və idarəetmə ilə bağlı boşluqlar dövlət üçün strateji risklər yaradır. AzDSI bu riskləri birbaşa ölçmə obyektinə çevirir;
- beynəlxalq indekslər əsasən müqayisəli reyting məqsədi daşıyır və dövlətlərin qərarvermə

ehtiyaclarına məhdud şəkildə cavab verir. AzDSI isə reytingdən çox daxili idarəetmə və prioritetləşdirmə aləti kimi işlənib. Bu, indeks nəticələrinin siyasət sənədlərinə, yol xəritələrinə və investisiya qərarlarına birbaşa inteqrasiyasına imkan yaradır;

- rəqəmsal suverenlik anlayışı sürətlə dəyişən texnoloji və geosiyasi mühitdə statik ölçmə alətləri ilə adekvat şəkildə qiymətləndirilə bilməz. AzDSI-nin modul və adaptiv strukturu yeni risklərin (məsələn, süni intellekt asılılıqları, platforma konsentrasiyası, bulud suverenliyi) indeksə inteqrasiyasını mümkün edir və onu uzunmüddətli monitoring alətinə çevirir.

BLOK 1. RƏQƏMSAL İNFRASTRUKTUR SUVERENLİYİ

Ölkənin fiziki və virtual rəqəmsal infrastruktur üzərində faktiki nəzarət dərəcəsinin qiymətləndirilməsi üçün altgöstəricilər və ölçmə parametrləri Cədvəl 4-də göstərilmişdir.

CƏDVƏL 4. RƏQƏMSAL İNFRASTRUKTUR SUVERENLİYİ BLOKUNUN ALTGÖSTƏRİCİLƏRİ VƏ ÖLÇMƏ PARAMETRLƏRİ

Altbloklar	Göstərici	Parametr
B1.1	Milli data-mərkəzlərin payı	Dövlət və əsas iqtisadi sektorların ümumi hesablama yükünün (“workload”) ölkə daxilində yerləşən data-mərkəzlərdə icra olunan hissəsi
B1.2	Telekom şəbəkələrinin idarə edilməsi	Core telekommunikasiya şəbəkələrinin hüquqi və əməliyyat idarəetmə səviyyəsi (milli nəzarət indeksi)
B1.3	Avadanlıq asılılığı	Server, şəbəkə və telekommunikasiya avadanlıqlarında idxal komponentlərinin nisbi payı
B1.4	Milli HPC / superkompüter	Yüksək performanslı hesablama infrastrukturunun mövcudluğu, hesablama gücü (PFLOPS) və strateji sektorlar üçün real istifadəyə açılış dərəcəsi

B1.1 dövlət və əsas iqtisadi sektorlar üzrə rəqəmsal xidmətlərin və məlumat emalının hansı hissəsinin (nisbi payı, %) ölkə daxilində yerləşən data-mərkəzlərdə icra olunduğunu ölçür. Milli data-mərkəzlərdə yerləşən “workload” payına uyğun şkala Cədvəl 5-də təqdim olunur.

CƏDVƏL 5. MİLLİ DATA-MƏRKƏZLƏRDƏ YERLƏŞƏN “WORKLOAD” PAYI ÜZRƏ BAL ŞKALASI

Nisbi “workload” payı	bal
≥ 80 %	100
60–79 %	75
40–59 %	50
20–39 %	25
< 20 %	0

B1.2 ölkənin telekommunikasiya şəbəkələrinin əsas (“core”) funksiyaları üzərində idarəetmə və nəzarət (“core” şəbəkələrin milli operatorların hüquqi tənzimləmə sferasına aid olması, şəbəkə idarəetməsinin yerli qurumlar tərəfindən həyata keçirilməsi) səviyyəsini ölçür. Burada avadanlığın mənşəyi deyil, idarəetmə səlahiyyətləri əsas amildir. Telekommunikasiya “core” şəbəkələri üzrə milli nəzarət səviyyəsinin qiymətləndirilməsi Cədvəl 6-da əks etdirilmişdir.

CƏDVƏL 6. TELEKOMMUNİKASIYA “CORE” ŞƏBƏKƏLƏRİ ÜZRƏ MİLLİ NƏZARƏT SƏVİYYƏSİNİN BAL ŞKALASI

milli nəzarət indeksi	bal
“Core” şəbəkə tam yerli nəzarətdədir	100
“Core” yerli, lakin texniki asılılıq yüksəkdir	75
“Core” qismən xarici nəzarətdədir	50
“Core” əsasən xaricdən idarə olunur	25
Nəzarət faktiki olaraq yoxdur	0

B1.3 rəqəmsal infrastrukturun əsas komponentləri (serverlər, şəbəkə və telekommunikasiya avadanlıqları) üzrə idxal olunan avadanlığın payını ölçür. İnfrastruktur avadanlıqlarında idxal asılılığı üzrə intervallar Cədvəl 7-də təqdim edilir.

CƏDVƏL 7. İNFRASTRUKTUR AVADANLIQLARINDA İDXAL ASILILIĞI ÜZRƏ BAL ŞKALASI

Avadanlığın idxal payı	bal
≤ 20 %	100
21–40 %	75
41–60 %	50
61–80 %	25
> 80 %	0

B1.4 ölkədə yüksək performanslı hesablama (High-Performance Computing, HPC) infrastrukturunun mövcudluğu və infrastrukturun dövlət qurumları, elmi-tədqiqat institutları, strateji sektorlar üçün real istifadəyə açıq olmasını ölçür və təklif olunan göstəricilər və ölçmə parametrləri Cədvəl 8-də sistemləşdirilmişdir.

CƏDVƏL 8. MİLLİ HPC/SUPERKOMPÜTER İNFRASTRUKTURUNUN MÖVCUDLUĞU VƏ İSTİFADƏYƏ AÇIQLIĞI ÜZRƏ BAL ŞKALASI

HPC mövcudluğu + istifadəyə açılışı	bal
Mövcud və geniş istifadəyə açıq	100
Mövcudd, lakin məhdud istifadə	75
Pilot və ya erkən mərhələ	50
Planlaşdırma mərhələsində	25
Mövcud deyil	0

B1 bloku üzrə yekun bal:

$$B_1 = \sum_{i=1}^4 w_{i1} \times b_{i1}$$

İlkin yanaşmada $w_{i1} = 0.25$ kimi götürülə, sonradan dəqiqləşdirilə bilər.

B1 bloku üzrə altbloklar üçün təqdim olunan ölçmə metodologiyası analoji olaraq digər bloklarda da tətbiq edilə bilər.

BLOK 2. MƏLUMAT SUVERENLİYİ

Məlumatın harada saxlanıldığı, kim tərəfindən idarə edildiyi və hüquqi çərçivə sferasının qiymətləndirilməsi üçün göstəricilər və ölçmə parametrləri Cədvəl 9-da sistemləşdirilmişdir [15].

CƏDVƏL 9. MƏLUMAT SUVERENLİYİ BLOKUNUN GÖSTƏRİCİLƏRİ VƏ ÖLÇMƏ PARAMETRLƏRİ

	Göstərici	Parametr
B2.1	Məlumatların idarə edilməsi	Hüquqi baza + texniki nəzarət mexanizmlərinin mövcudluğu və effektivliyi
B2.2	Milli reyestrlər və e-hökumət	Dövlət xidmətlərinin rəqəmsallaşma və mərkəzləşmə səviyyəsi
B2.3	Kritik “data”nın ölkə daxilində saxlanması	Dövlət və özəl sektor üzrə lokal saxlanma payı
B2.4	Xarici bulud dominantlığı	Xarici bulud xidmətlərinin bazar payı və ya dövlət sektorunda istifadə payı

BLOK 3. TEXNOLOJİ SUVERENLİK

Əsas texnoloji sahələr üzrə əvəzləmə və lokal inkişaf potensialının qiymətləndirilməsi üçün əsas göstəricilər və ölçmə parametrləri Cədvəl 10-da göstərilmişdir.

CƏDVƏL 10. TEXNOLOJİ SUVERENLİK BLOKUNUN GÖSTƏRİCİLƏRİ VƏ ÖLÇMƏ PARAMETRLƏRİ

	Göstərici	Parametr
B3.1	İdخال proqram və hardware payı	Əsas sistem proqram təminatında və infrastruktur avadanlığında idخال komponentlərinin nisbi payı
B3.2	Yerli OS, çip, AI təşəbbüsləri	Milli texnoloji məhsulların mövcudluğu və tətbiq səviyyəsi (müvcudluq + bazar/pay tətbiqi indeksi)
B3.3	Big Tech-dən asılılıq	Dövlət və strateji sektor xidmətlərində qlobal platforma/bulud/süni intellekt provayderlərinin istifadə payı
B3.4	Platforma müstəqilliyi	İctimai kommunikasiya və dövlət rəqəmsal xidmətlərində yerli/regional platformaların istifadə payı

BLOK 4. TƏNZİMLƏYİCİ SUVERENLİK

Dövlətin rəqəmsal mühit üzrə mövcud qanunvericilik bazası və idarəetmə mexanizmlərinin qiymətləndirilməsi məqsədilə zəruri göstəricilər və ölçmə parametrləri Cədvəl 11-də təqdim olunur.

CƏDVƏL 11. TƏNZİMLƏYİCİ SUVERENLİK BLOKUNUN GÖSTƏRİCİLƏRİ VƏ ÖLÇMƏ PARAMETRLƏRİ

	Göstərici	Parametr
B4.1	Rəqəmsal qanunvericilik	Rəqəmsal sahəni əhatə edən normativ aktların əhatəlilik və uyğunluq indeksi
B4.2	Texniki nəzarət mexanizmləri	Qanunların faktiki icra və monitorinq səviyyəsi
B4.3	Antimonopol imkanlar	Qlobal rəqəmsal platformalara qarşı tətbiq edilə bilən rəqabət və tənzimləmə alətlərinin effektivliyi

B4.4	Transsərhəd “data” axınlarına nəzarət	Transsərhəd məlumat ötürülməsi üzrə real nəzarət və icazə mexanizmlərinin tətbiq səviyyəsi
------	---------------------------------------	--

BLOK 5. KADRLAR VƏ İNNOVASIYA

Uzunmüddətli rəqəmsal müstəqillik potensialının qiymətləndirilməsi üçün göstəricilər Cədvəl 12-də əks edilmişdir.

CƏDVƏL 12. KADRLAR VƏ İNNOVASIYA BLOKUNUN GÖSTƏRİCİLƏRİ VƏ ÖLÇMƏ PARAMETRLƏRİ

	Göstərici	Parametr
B5.1	IT mütəxəssislərinin sayı	100 min nəfərə düşən IT mütəxəssislərinin sayı və illik artım tempi
B5.2	Beyin axını riski	IT mütəxəssislərinin xaricə miqrasiya göstəricisi və ya kadr balansı
B5.3	R&D və innovasiya ekosistemi	ÜDM-də IT və rəqəmsal sahəyə yönələn R&D xərclərinin payı
B5.4	Startaplar və patentlər	1 milyon nəfərə düşən texnoloji startap sayı və ya İKT üzrə patent müraciətlərinin sayı

BLOK 6. DAYANIQLILIQ

Rəqəmsal ekosistemin kibereyanıqlılığını qiymətləndirmək üçün göstəricilər və ölçmə parametrləri Cədvəl 13-də ümumiləşdirilmişdir.

CƏDVƏL 13. DAYANIQLILIQ BLOKUNUN GÖSTƏRİCİLƏRİ VƏ ÖLÇMƏ PARAMETRLƏRİ

	Göstərici	Parametr
B6.1	Geosiyasi və sanksiya riskləri	Strateji texnologiyalarda sanksiya və təcizat zənciri risklərinə məruz qalma dərəcəsi
B6.2	İnformasiya manipulyasiyası riski	Xarici platformaların informasiya məkanındakı payı və dezinformasiya insidentlərinin intensivliyi
B6.3	Kiberhücumlara cavab	Milli CERT/SOC imkanları, insidentlərə reaksiya müddəti və beynəlxalq reytinglərdə mövqe
B6.4	Alternativ ssenarilər	Fövqəladə hallarda alternativ infrastruktur və davamlılıq planlarının mövcudluq və tətbiq indeksi

Blokların mühümlük dərəcəsini müəyyənləşdirmək üçün 3 meyar əsasında “çəkilər” təyin edirik:

- 1) *Kritiklik* – dövlətin funksiyalarına birbaşa təsir;
- 2) *Əvəzləmə çətinliyi* – qısa müddətdə alternativ variantın mümkünlüyü;
- 3) *Sistem riski* – sistemin funksionallığının pozulmasının digər blokların funksionallığına təsiri.

Bloklar üzrə çəkilər Cədvəl 14-də kimi təyin olunur:

CƏDVƏL 14. AZRSİ BLOKLARI ÜZRƏ ÇƏKİ ƏMSALLARI

Blok	Təsviri	Çəki (w_j)
B1	Rəqəmsal infrastruktur suverenliyi	0.20
B2	Məlumat suverenliyi	0.15
B3	Texnoloji suverenlik	0.20
B4	Tənzimləyici suverenlik	0.15
B5	Kadrlar və innovasiya	0.10
B6	Dayanıqlılıq (kiberdayanıqlılıq)	0.20
Cəmi		1.00

B1, B3, B6 - kritik sistem blokları, B2, B4 - idarəetmə və hüquqi nəzarət, B5 - uzunmüddətli struktur faktor.

Blok daxili çəkilər:

$$B_j = \sum_{i=1}^n w_{ij} \times b_{ij}, j = 1, \dots, 6$$

w_{ij} – göstəricilərin çəkisi, b_{ij} – i-ci göstərici,

Blokdakı göstəricilər eynigüclü hesab olunduğu təqdirdə:

$$\sum_{i=1}^n w_{ij} = 1 \quad w_i = 1/n_i$$

Ekspert əsaslı qiymətləndirməyə ehtiyac olduqda, məsələn, çəkilər aşağıdakı kimi seçilə bilər:

B3.1 (idxal payı) → 0,35

B3.2 (yerli təşəbbüslər) → 0,20

B3.3 (Big Tech asılılığı) → 0,30

B3.4 (platforma müstəqilliyi) → 0,15.

AzRSİ-nin hesablama düsturu:

$$AzDSI = \sum_{j=1}^n w_j \times B_j$$

burada w_j – blokun çəkisi, B_j – hər blokun ümumi balı,

$$\sum_{j=1}^n w_j = 1$$

AzRSİ üçün hesablanmış ümumi balın interpretasiyası Cədvəl 15-də təqdim olunur.

CƏDVƏL 15. AZRSİ BALININ İNTERPRETASIYA ŞKALASI

DSI balı	Şərh
0–30	Kritik asılılıq
31–50	Zəif suverenlik
51–65	Keçid mərhələsi
66–80	Funksional suverenlik
81–100	Yüksək rəqəmsal suverenlik

AzDSI-nin mövcud indekslərdən metodoloji fərqi aşağıdakılardan ibarətdir:

1) AzDSI rəqəmsal suverenliyi nəticə göstəricisi kimi deyil, idarəolunan sistem riski və idarəetmə qabiliyyəti kimi konseptuallaşdırır. Mövcud indekslərin əksəriyyəti “nə qədər rəqəmsallaşmış?” sualına cavab verdiyi halda, AzDSI “dövlət bu rəqəmsal asılılıqları nə dərəcədə idarə edə bilir?” sualını əsas götürür. Bu yanaşma rəqəmsal suverenliyi texnoloji səviyyədə çıxararaq strateji idarəetmə kateqoriyasına çevirir.

2) AzDSI metodologiyası risk əsaslı blok strukturu üzərində qurulub. Altı blok (rəqəmsal infrastruktur, məlumat, əsas texnologiyalar, tənzimləyici potensial, insan kapitalı və kiberdayanıqlılıq) bir-birindən müstəqil göstəricilər kimi deyil, sistem qarşılıqlı asılılıqları nəzərə alınmaqla işlənib. Bu

yanaşma sistem səviyyəsində zəifliklərin digər sahələrə ötürülmə riskini ölçməyə imkan verir ki, bu xüsusiyyət mövcud indekslərdə adətən nəzərə alınmır.

3) AzDSI normativ meyarlardan çox ölçüləbilən indikatorlara üstünlük verir. Bir çox beynəlxalq indekslər qanunvericiliyin mövcudluğunu və ya siyasət sənədlərinin qəbulunu yüksək bal kimi qiymətləndirdiyi halda, AzDSI həmin mexanizmlərin icra edilə bilmə qabiliyyətini, qurumlararası koordinasiyanı və praktik tətbiq potensialını ölçməyə çalışır. Bu yanaşma “kağız üzərində suverenlik” ilə real idarəetmə imkanları arasında fərqi üzə çıxarır.

AzRSİ bloklarının qiymətini “pilot” məqsədilə etibarlı beynəlxalq mənbələrdən götürülən proksi-göstəricilər əsasında (0–100 şkalası) hesablamaq üçün Cədvəl 16-dakı müvafiq proksi indikatorlardan istifadə etmək olar.

CƏDVƏL 16. AZRSİ-NİN PİLOT HESABLAMASI ÜÇÜN PROKSİ İNDİKATORLAR VƏ BLOK BALLARI

AzDSI bloku	Proksi indikator (mənbə)	İl	bal
Blok 1. Rəqəmsal infrastruktur suverenliyi	ITU ICT Development Index (IDI) “Meaningful connectivity” score	2024	80,4
Blok 2. Məlumat suverenliyi	UN EGDİ (E-Government Development Index)	2024	76,07
Blok 3. Texnoloji suverenlik	WIPO Global Innovation Index (GII) overall score	2024	21,3
Blok 4. Tənzimləyici suverenlik	World Bank WGI Government Effectiveness – Percentile Rank	2023	50,47
Blok 5. İnsan kapitalı	Oxford Insights Government AI Readiness Index score	2024	39,92
Blok 6. Kiberdayanıqlılıq	ITU Global Cybersecurity Index (GCI) score	2024	93,76

Nəticə: AzRSİ (pilot) = 60.065/100

$(0.20 \times 80.4 + 0.15 \times 76.07 + 0.20 \times 21.3 + 0.15 \times 50.47 + 0.10 \times 39.92 + 0.20 \times 93.76 = 62.065$, “keçid mərhələsi”)

Real milli statistik məlumatların tam əlçatan olmadığı mərhələdə Cədvəl 16-da təqdim edilən proksi göstəricilər AzRSİ metodologiyasının ilkin sınaq hesablaması üçün istifadə edilmişdir. Bu göstəricilər rəqəmsal suverenliyin ayrı-ayrı bloklarını birbaşa və tam ölçməyə də, beynəlxalq səviyyədə tanınan, müqayisə oluna bilən və müntəzəm yenilənən indekslərə əsaslandığı üçün pilot qiymətləndirmənin obyektivliyini qismən təmin edir. Bununla belə, proksi göstəricilər metodologiyasının yekun empirik təsdiqi kimi deyil, real milli məlumatlar formalaşana qədər tətbiq edilən keçid ölçmə aləti kimi qiymətləndirilməlidir. AzRSİ hesablanması üçün gələcək mərhələdə milli data-mərkəzlərdə yerləşən “workload” payı, idxal proqram və avadanlıq komponentlərinin faktiki nisbəti, dövlət sektorunda xarici bulud və platforma istifadəsi, kritik məlumatların lokal saxlanma səviyyəsi və kiberinsidentlərə reaksiya göstəriciləri kimi birbaşa milli indikatorların toplanması zəruridir.

Qeyd: Pilot mərhələsində Blok5 üçün yalnız “Government AI Readiness Index” göstəricisindən istifadə edilmişdir. Bu seçim bloklararası indikator təkrarlanmasının (“double

counting”) qarşısını almaq və insan kapitalını kiberdayanıqlılıq blokundan konseptual olaraq ayırmaq məqsədi daşıyır. AzRSİ metodologiyasında isə Blok5 insan kapitalının həm ümumi rəqəmsal idarəetmə qabiliyyəti, həm də kibertəhlükəsizlik üzrə komponentlərini əhatə edən çoxindikatorlu ölçmə ilə hesablanmalıdır.

Cədvəl 16-da təqdim olunan proksi-göstəricilər əsasında eyni çəki mexanizmini Türkiyə və Rusiyanın beynəlxalq indikatorlarına tətbiq etsək, pilot hesablama nəticəsində Türkiyə üzrə AzRSİ göstəricisi $70.96/100$ ($0.20 \times 87.50 + 0.15 \times 89.13 + 0.20 \times 39.00 + 0.15 \times 41.51 + 0.10 \times 60.63 + 0.20 \times 100.00 = 70.96$), Rusiya üzrə isə $65.72/100$ ($0.20 \times 90.60 + 0.15 \times 85.33 + 0.20 \times 29.70 + 0.15 \times 26.42 + 0.10 \times 64.72 + 0.20 \times 92.12 = 65.72$) kimi müəyyən edilir. Bu nəticələr göstərir ki, Türkiyə proksi-hesablama əsasında “funksional suverenlik” intervalına daxil olur, Rusiya isə “keçid mərhələsi” ilə “funksional suverenlik” sərhədində yerləşir. Hər iki ölkədə yüksək rəqəmsal infrastruktur və kiberdayanıqlılıq göstəriciləri ümumi bala müsbət təsir göstərsə də, texnoloji suverenlik və tənzimləyici effektivlik üzrə nisbətən zəif göstəricilər yekun indeks nəticəsini məhdudlaşdırır. Bu isə proksi-hesablamının ölkələr üzrə ümumi müqayisə aparmaq üçün faydalı olduğunu göstərir.

NƏTİCƏ

Bu tədqiqat rəqəmsal suverenlik anlayışının normativ və bu tədqiqat rəqəmsal suverenlik anlayışının normativ və siyasi diskurs çərçivəsindən çıxarılaq ölçülə, müqayisə oluna bilən və idarə olunan analitik alətə çevrilməsinin zərurətini əsaslandırır. Aparılmış müqayisəli təhlil göstərir ki, mövcud yanaşmalar: konseptual-strateji (WIK-Consult), indikator-əsaslı analitik (SDIA) və empirik-istifadə yönümlü (DSI) modellər ayrı-ayrılıqda rəqəmsal suverenliyin müxtəlif ölçülərini əhatə etsə də, onların inteqrasiyası daha balanslı və funksional qiymətləndirmə çərçivəsi formalaşdırır.

Təklif olunan RSM və onun əsasında işlənmiş AzRSİ rəqəmsal infrastruktur, məlumat, texnologiya, tənzimləmə, insan kapitalı və kiberdayanıqlılıq komponentlərini vahid metodoloji sistem daxilində birləşdirir. Risk-əsaslı çəkili mexanizmi isə kritik struktur asılılıqların daha dəqiq identifikasiyasına və prioritetləşdirilməsinə imkan verir. Bu yanaşma rəqəmsal suverenliyi yalnız hüquqi müstəvidə deyil, həm də faktiki texnoloji və əməliyyat imkanları kontekstində qiymətləndirməyə şərait yaradır.

Tədqiqatın əsas məhdudiyyəti real milli statistik məlumatların əlçatan olmaması və pilot hesablamının beynəlxalq proksi-göstəricilərə əsaslanmasıdır. Gələcək mərhələdə AzRSİ-nin daha dəqiq hesablanması üçün milli data-mərkəzlərdə yerləşən “workload” payı, dövlət sektorunda xarici bulud istifadəsi, idxal proqram təminatı və avadanlıq payı, kritik məlumatların lokal saxlanma səviyyəsi və kibersidentlərə reaksiya müddəti kimi birbaşa indikatorların toplanması zəruridir.

Azərbaycan üzrə aparılmış ilkin analitik qiymətləndirmə göstərir ki, əsas zəifliklər texnoloji və platforma asılılığı istiqamətində cəmlənir. Hüquqi baza formalaşsa da, real “data”

axınları, bulud infrastrukturu və əsas texnoloji komponentlər üzrə xarici asılılıq davam edir. Bu isə rəqəmsal ekosistemin geosiyasi və bazar dəyişikliklərinə qarşı həssaslığını artırır. Eyni zamanda, milli data-mərkəzlərin mövcudluğu, e-hökumət infrastrukturu və artan İT kadr potensialı funksional suverenliyin gücləndirilməsi üçün baza yaradır.

AzRSİ modeli qərarvericilər üçün aşağıdakı üstünlükləri təmin edə bilər:

- rəqəmsal asılılıqların struktur xəritələndirilməsi;
- infrastruktur və texnoloji investisiyaların prioritetləşdirilməsi;
- tənzimləmə və idarəetmə boşluqlarının identifikasiyası;
- uzunmüddətli rəqəmsal strategiyaların effektivliyinin ölçülməsi.

Beləliklə, tədqiqatın əsas töhfəsi rəqəmsal suverenliyin Azərbaycan kontekstində ilk dəfə çoxbloklı, risk-əsaslı və çəkili indeks modeli kimi konseptuallaşdırılmasıdır. Rəqəmsal suverenlik “tam müstəqillik” konsepsiyası kimi deyil, idarə olunan asılılıqların optimallaşdırılması və strateji dayanıqlılığın təmin edilməsi prosesi kimi nəzərdən keçirilməlidir. Təklif olunan model bu prosesi sistemləşdirmək və mərhələli şəkildə ölçmək üçün metodoloji əsas təqdim edir. Gələcək tədqiqatlarda indeksin empirik məlumatlarla geniş tətbiqi, beynəlxalq müqayisələrin aparılması və zaman üzrə dinamik analiz rəqəmsal suverenlik siyasətinin daha effektiv formalaşdırılmasına töhfə verə bilər.

ƏDƏBİYYAT

- [1] J. Pohle and T. Thiel, “Digital sovereignty,” *Internet Policy Review*, vol. 9, no. 4, 2020, doi: 10.14763/2020.4.1532.
- [2] S. Couture and S. Toupin, “What does the notion of ‘sovereignty’ mean when referring to the digital?” *New Media & Society*, 2019.
- [3] M. L. Mueller, “Digital sovereignty and its discontents,” *Telecommunications Policy*, 2022.
- [4] “Digital sovereignty assessment matrix,” Available: <https://ided.digital/governments/policy-tools/digital-sovereignty-assessment-matrix>
- [5] “Digital Sovereignty Report,” Available: https://www.wik.org/fileadmin/files/_migrated/news_files/Digital_Sovereignty_Report.pdf
- [6] “EIT Digital Data Sovereignty Report,” Available: <https://www.eit.europa.eu/sites/default/files/eit-digital-data-sovereignty-full-report.pdf>
- [7] <https://link.springer.com/article/10.1007/s44206-024-00146-7>
- [8] “Digital Sovereignty,” *Internet Society*, 2022. Available: <https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf>
- [9] “Digital Sovereignty Observatory,” Available: <https://www.digitalsovereigntyobservatory.org/>
- [10] European Commission document, Available: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en
- [11] “Sustainable Digital Infrastructure Alliance (SDIA) profile,” Available: <https://www.worldbenchmarkingalliance.org/profile/sustainable-digital-infrastructure-alliance-ev-sdia>
- [12] “Digital sovereignty assessment matrix,” Available: <https://ided.digital/governments/policy-tools/digital-sovereignty-assessment-matrix>

- [13] “Nextcloud Digital Sovereignty Initiative,” Available: <https://dsi.nextcloud.com>
- [14] A. Chander and U. P. Lê, “Data nationalism,” *Emory Law Journal*, vol. 64, no. 3, 2015. Available: <https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2>
- [15] OECD, “A preliminary mapping of data localisation measures,” 2022. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/06/a-preliminary-mapping-of-data-localisation-measures_6ac088e7/c5ca3fed-en.pdf
- [16] “Digital Sovereignty from the BRICS,” *CyberBRICS*, 2024. Available: https://cyberbrics.info/wp-content/uploads/2024/05/Pre-print-version-Digital-Sovereignty-from-the-BRICS_Structuring-Self-determination-Cybersecurity-and-Control-1.pdf
- [17] “China’s vision of cyber sovereignty,” *Red Sky Alliance*. Available: <https://redskyalliance.org/xindustry/china-s-vision-of-cyber-sovereignty>
- [18] “Digital sovereignty article,” *RUDN Journal of Political Science*. Available: <https://journals.rudn.ru/political-science/article/view/2654>
- [19] “Cybersecurity Law of the People’s Republic of China,” Available: https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China
- [20] “AzInTelecom builds first supercomputer center in Azerbaijan,” Available: <https://azintelecom.az/az/news/azintelecom-azerbaycanda-ilk-superkomputer-merkezi-qurub>

Azerbaijan Digital Sovereignty Index: An Analytical and Methodological Approach

Lala Karimova

Ministry of Digital Development and Transport of the Republic of Azerbaijan, Baku, Azerbaijan

Abstract– This article analyzes approaches aimed at transforming the concept of digital sovereignty into a measurable and manageable instrument. The study compares conceptual and indicator-based models applied in international practice, identifying their strengths and limitations. The article presents the methodology of Azerbaijan’s Digital Sovereignty Index (AzDSI). The proposed model enables an integrated assessment of digital infrastructure, data, technology, regulation, human capital, and cyber resilience.

Keywords– digital sovereignty; digital sovereignty matrix; digital sovereignty index; cyber resilience.