Kibersuverenlik Konsepsiyası və Onun Dövlət Təhlükəsizlik Sistemində Rolu

Ayna Əlixanova
Nizami Gəncəvi adına Milli Azərbaycan Ədəbiyyatı Muzeyi, Bakı, Azərbaycan
aynaalixan@gmail.com

***Xülasə*— Məqalədə dövlətin kibersuverenliyinin təmin olunmasının elmi və praktik problemləri təhlil olunur. Müasir rəqəmsal transformasiya şəraitində kiberməkanın dövlət suverenliyinin yeni ölçüsünə çevrildiyi əsaslandırılır. Kibersuverenlik anlayışının nəzəri əsasları araşdırılır, onun normativ, texnoloji, informasiya və iqtisadi komponentləri müəyyən edilir. Beynəlxalq hüquqda kiberməkanın hüquqi statusu ilə bağlı mövcud boşluqlar, terminoloji qeyri-müəyyənlik, texnoloji asılılıq və yurisdiksiya problemləri elmi müstəvidə qiymətləndirilir. Eyni zamanda dövlətlərin qarşılaşdığı praktik çağırışlar – kiberhücumlar, dezinformasiya, transmilli platformaların dominantlığı və təhlükəsizliklə insan hüquqları arasında balans məsələsi təhlil olunur. Azərbaycan Respublikasının kibertəhlükəsizlik siyasəti kontekstində milli prioritetlər və perspektiv istiqamətlər müəyyən edilir. Nəticə etibarilə, kibersuverenliyin milli təhlükəsizliyin mühüm elementi kimi strateji əhəmiyyəti əsaslandırılır.**

Açar sözlər*— *kibersuverenlik; kibertəhlükəsizlik; informasiya təhlükəsizliyi; rəqəmsal transformasiyalar; kiberhücum; dezinformasiya; transmilli platformalar.

I. GİRİŞ

XXI əsrdə rəqəmsallaşma prosesinin intensivləşməsi qlobal siyasi-iqtisadi sistemin strukturunu köklü şəkildə transformasiya edərək dövlətlərin fəaliyyət mühitini yeni reallıqlarla üz-üzə qoymuşdur. İnformasiya-kommunikasiya texnologiyalarının sürətli inkişafı nəticəsində kiberməkan artıq yalnız texniki platforma kimi deyil, həm də dövlətlərarası qarşılıqlı təsirin, geosiyasi rəqabətin, iqtisadi inteqrasiyanın və strateji idarəetmənin əsas mühitlərindən biri kimi çıxış edir [1, 2].

Müasir şəraitdə kiberməkanın funksional əhəmiyyəti onun çoxşaxəli xarakteri ilə müəyyən olunur. Bir tərəfdən bu mühit qlobal informasiya mübadiləsini və iqtisadi fəaliyyətin sürətlənməsini təmin edir, digər tərəfdən isə yeni təhlükəsizlik risklərinin yaranmasına səbəb olur. Bu baxımdan kiberməkan həm inkişaf imkanlarının, həm də qeyri-ənənəvi təhlükələrin paralel mövcud olduğu kompleks sistem kimi qiymətləndirilə bilər.

Ənənəvi suverenlik konsepsiyası Vestfaliya sisteminə əsaslanaraq dövlətin müəyyən ərazi daxilində ali hakimiyyətini ifadə edirdi. Bu yanaşma dövlətin ərazi bütövlüyü, siyasi müstəqilliyi və daxili işlərinə xarici müdaxilənin yolverilməzliyi prinsiplərinə əsaslanırdı. Lakin qloballaşma və rəqəmsallaşma prosesləri nəticəsində informasiya axınlarının sərhədsiz xarakter alması, transmilli şəbəkələrin və rəqəmsal platformaların formalaşması bu konsepsiyanın funksional məhdudiyyətlərini üzə çıxarmışdır [3].

Belə ki, müasir dövrdə informasiya resursları və rəqəmsal infrastrukturlar dövlət sərhədlərindən kənarda yerləşə, lakin həmin dövlətin iqtisadi və siyasi sisteminə birbaşa təsir göstərə bilər. Bu isə suverenlik anlayışının yalnız fiziki ərazi ilə məhdudlaşdırılmasının qeyri-kafi olduğunu göstərir və onun yeni – rəqəmsal ölçüsünün nəzərə alınmasını zəruri edir.

Bu kontekstdə kibersuverenlik anlayışı dövlətin yalnız fiziki deyil, həm də virtual məkan üzərində hakimiyyət və nəzarət imkanlarını ifadə edən yeni konseptual kateqoriya kimi formalaşmışdır. Bu anlayış dövlətin rəqəmsal mühitdə təhlükəsizliyini təmin etməklə yanaşı, onun siyasi müstəqilliyinin, iqtisadi dayanıqlılığının və informasiya mühitinin qorunmasına xidmət edir [4, 5].

Eyni zamanda kibersuverenlik anlayışı dövlətin rəqəmsal transformasiya proseslərinə uyğunlaşma səviyyəsini və onun qlobal rəqəmsal sistemdə mövqeyini müəyyən edən əsas indikatorlardan biri kimi çıxış edir. Bu baxımdan kibersuverenlik yalnız müdafiə xarakterli konsepsiya deyil, həm də dövlətin rəqəmsal inkişaf strategiyasının ayrılmaz tərkib hissəsidir.

II. KİBERSUVERENLİYİN NƏZƏRİ-KONSEPTUAL ƏSASLARI

Kibersuverenlik konsepsiyası müasir beynəlxalq münasibətlər nəzəriyyəsində suverenliyin evolyusion inkişaf mərhələsini əks etdirən fundamental kateqoriyalardan biri kimi çıxış edir. Bu yanaşma dövlətin kiberməkanda müstəqil qərarvermə qabiliyyətini, informasiya axınlarına nəzarət imkanlarını və rəqəmsal resursların strateji idarə olunmasını özündə ehtiva edir [6,7]. Müasir elmi yanaşmalara əsasən kibersuverenlik yalnız hüquqi və texnoloji fenomen deyil, eyni zamanda siyasi hakimiyyətin rəqəmsal mühitdə realizə olunma forması kimi də qiymətləndirilir. Bu baxımdan kibersuverenlik dövlətin milli maraqlarını kiberməkanda qorumaq qabiliyyətini və bu sahədə müstəqil siyasət yürütmək imkanlarını əks etdirir. Elmi ədəbiyyatda kibersuverenlik çoxkomponentli sistem kimi xarakterizə olunur və onun struktur elementləri aşağıdakı kimi təsnif edilir:

Normativ komponent

Bu komponent dövlətin kiberməkanda hüquqi tənzimləmə mexanizmlərini, milli qanunvericilik bazasını və beynəlxalq hüquq normaları ilə qarşılıqlı əlaqəsini əhatə edir. Normativ komponent kiberməkanın hüquqi rejiminin formalaşdırılmasında və dövlətin bu mühitdə hüquqi

DOI: 10.25045/cyber.gov.2026.25

suverenliyinin təmin olunmasında həlledici rol oynayır [8].

Bununla yanaşı, normativ komponent yalnız daxili hüquqla məhdudlaşmır, həm də beynəlxalq hüquq sistemində dövlətlərin öhdəlikləri və hüquqlarının müəyyənləşdirilməsini əhatə edir.

Texnoloji komponent

Texnoloji komponent milli informasiya infrastrukturu, data mərkəzləri, şəbəkə sistemləri və proqram təminatı üzərində nəzarəti ifadə edir. Texnoloji müstəqillik səviyyəsi dövlətin kibersuverenliyinin əsas indikatorlarından biri hesab olunur [9].

Bu komponent çərçivəsində dövlətin öz texnoloji resurslarını inkişaf etdirməsi, yerli innovasiya ekosisteminin formalaşdırılması və xarici texnologiyalardan asılılığın azaldılması xüsusi əhəmiyyət kəsb edir.

İnformasiya komponenti

Bu komponent informasiya təhlükəsizliyi, məlumatların qorunması və dezinformasiyaya qarşı mübarizə mexanizmlərini əhatə edir. İnformasiya mühiti üzərində nəzarət dövlətin ictimai sabitliyinin, sosial harmoniyanın və siyasi legitimliyin qorunmasında mühüm rol oynayır [10].

Eyni zamanda informasiya komponenti strateji kommunikasiya siyasəti ilə sıx bağlıdır və dövlətin informasiya müharibəsi şəraitində effektiv fəaliyyət göstərməsini təmin edir.

İqtisadi komponent

Rəqəmsal iqtisadiyyatın inkişafı şəraitində dövlətin iqtisadi suverenliyi getdikcə daha çox texnoloji resurslardan, böyük verilənlərdən (big data) və rəqəmsal platformalardan asılı olur. Bu baxımdan iqtisadi komponent kibersuverenliyin ayrılmaz hissəsi kimi çıxış edir [11].

Rəqəmsal bazarların tənzimlənməsi, milli iqtisadi maraqların qorunması və rəqəmsal xidmətlər üzərində nəzarət bu komponentin əsas istiqamətlərini təşkil edir.

Kibersuverenlik konsepsiyasının nəzəri izahında müxtəlif beynəlxalq münasibətlər nəzəriyyələri mühüm rol oynayır.

Realist yanaşma

Bu yanaşmaya görə kiberməkan dövlətlərarası güc mübarizəsinin yeni arenasıdır və burada üstünlük əldə etmək milli təhlükəsizlik baxımından strateji əhəmiyyət daşıyır. Bu yanaşma kiberməkanı rəqabət və qarşıdurma mühiti kimi qiymətləndirir [12].

Liberal yanaşma

Liberal yanaşma isə kiberməkanı qlobal əməkdaşlıq və qarşılıqlı asılılıq mühiti kimi izah edir. Bu yanaşmaya görə beynəlxalq təşkilatlar, çoxtərəfli razılaşmalar və normativ mexanizmlər kiberməkanda sabitliyin təmin olunmasında mühüm rol oynayır.

Konstruktivist yanaşma

Konstruktivist yanaşma kiberməkanın sosial konstruksiya kimi formalaşdığını və burada normativ dəyərlərin, identikliklərin və diskursların mühüm rol oynadığını vurğulayır.

Beləliklə, kibersuverenlik konsepsiyası müxtəlif nəzəri yanaşmaların kəsişməsində formalaşan kompleks və dinamik anlayış kimi çıxış edir və onun dərk edilməsi müasir beynəlxalq münasibətlərin təhlilində xüsusi əhəmiyyət kəsb edir.

III. KİBERSUVERENLİYİN TƏMİNİNDƏ MÖVCUD PROBLEMLƏR

Kibersuverenliyin nəzəri əsaslarının formalaşması prosesi mürəkkəb və çoxölçülü xarakter daşıyır. Bu sahədə mövcud olan fundamental elmi problemlər yalnız nəzəri diskussiyalarla məhdudlaşmır, eyni zamanda dövlətlərin praktik siyasət formalaşdırma və qərarvermə proseslərinə də birbaşa təsir göstərir. Müasir tədqiqatlar göstərir ki, kibersuverenliyin konseptual çərçivəsinin tam şəkildə müəyyənləşdirilməməsi onun tətbiqi mexanizmlərinin effektivliyini məhdudlaşdıran əsas amillərdən biridir.

Terminoloji qeyri-müəyyənlik kibersuverenlik

Bu ən mühüm problemlərindən biri kimi çıxış edir. “Kibersuverenlik”, “rəqəmsal suverenlik” və “informasiya suverenliyi” anlayışları çox vaxt paralel və ya sinonim kimi istifadə olunsa da, onların məzmunu və tətbiq sahələri arasında əhəmiyyətli fərqlər mövcuddur. Müxtəlif elmi məktəblər və tədqiqatçılar tərəfindən təqdim olunan fərqli yanaşmalar vahid terminoloji bazanın formalaşmasını çətinləşdirir və nəticə etibarilə bu sahədə konseptual qeyri-müəyyənlik yaradır [13]. Bu isə həm nəzəri model quruculuğuna, həm də normativ-hüquqi tənzimləmə proseslərinə mənfi təsir göstərir.

Yurisdiksiya problemi

Kiberməkanın sərhədsiz və qeyri-fiziki təbiətindən irəli gələn əsas çağırışlardan biridir. Ənənəvi hüquq sistemləri ərazi prinsipi üzərində qurulduğu halda, kiberməkanda fəaliyyət göstərən subyektlərin coğrafi yerləşməsi və hüquqi statusu çox zaman qeyri-müəyyən olur. Bu vəziyyət dövlətlərin hüquqi səlahiyyətlərinin tətbiqində çətinliklər yaradır, xüsusilə də transsərhəd kiberinsidentlərin araşdırılması və hüquqi məsuliyyətin müəyyənləşdirilməsi prosesində ciddi problemlər ortaya çıxarır [14].

Hüquqi fragmentasiya

Beynəlxalq hüquq sistemində kiberməkanla bağlı vahid və məcburi normativ çərçivənin olmaması ilə xarakterizə olunur. Mövcud beynəlxalq sənədlər və təşəbbüslər, o cümlədən müxtəlif regional və çoxtərəfli razılaşmalar, ümumi prinsipləri müəyyən etsə də, onların tətbiqi vahid mexanizmə əsaslanmır. Bu isə dövlətlər arasında fərqli hüquqi yanaşmaların formalaşmasına, normativ parçalanmaya və hüquqi qeyri-müəyyənliyə səbəb olur [15].

Texnoloji asılılıq və rəqəmsal asimmetriya

Müasir qlobal sistemdə kibersuverenliyin təmin olunmasına təsir edən mühüm amillərdən biridir. Qlobal texnologiya şirkətlərinin dominant mövqeyi və inkişaf etmiş ölkələrin texnoloji üstünlüyü digər dövlətlərin rəqəmsal müstəqilliyini məhdudlaşdırır. Bu vəziyyət rəqəmsal bərabərsizliyi dərinləşdirir və kiberməkanda güc balansının qeyri-bərabər şəkildə formalaşmasına səbəb olur [16]. Nəticədə bəzi dövlətlər kiberməkan üzərində tam nəzarət imkanlarına malik olduğu halda, digərləri texnoloji asılılıq vəziyyətində qalır.

Atribusiya problemi

Kiber hücumların mənbəyinin dəqiq müəyyənləşdirilməsi də kibersuverenliyin təminində mühüm elmi və praktik çətinliklərdən biridir. Kiberhücumların anonim xarakter daşıması və texniki maskalanma imkanları hücumun mənbəyini müəyyən etməyi çətinləşdirir və bu, hüquqi məsuliyyətin tətbiqini mürəkkəbləşdirir.

IV. PRAKTİK ÇAĞIRIŞLAR

Müasir beynəlxalq təhlükəsizlik mühitində kiberməkan qeyri-ənənəvi təhlükələrin formalaşdığı əsas mühitlərdən biri kimi çıxış edir. Bu mühitdə yaranan çağırışlar dövlətlərin milli təhlükəsizlik sistemlərinə çoxşaxəli təsir göstərir və onların adaptiv idarəetmə mexanizmlərinə ehtiyacını artırır.

Kiberhücumlar

Müasir dövrdə ən ciddi təhlükələrdən biri hesab olunur. Kritik informasiya infrastrukturlarına – enerji, nəqliyyat, bank və rabitə sistemlərinə yönəlmiş hücumlar dövlətlərin iqtisadi sabitliyini, ictimai xidmətlərin davamlılığını və sosial rifahını birbaşa təhdid edir [17]. Bu hücumların miqyası və mürəkkəbliyi artdıqca, dövlətlərin müdafiə və reaksiya imkanlarının da mütənasib şəkildə inkişaf etdirilməsi zəruri olur.

Dezinformasiya və informasiya manipulyasiyası

Yeni dövrdə informasiya müharibəsi müasir təhlükəsizlik mühitində ən təsirli və geniş tətbiq olunan əsas alətlərdən biri kimi ön plana çıxır. Sosial media platformaları vasitəsilə yayılan yanlış və ya manipulyativ məlumatlar ictimai rəyə təsir göstərərək siyasi proseslərin legitimliyini zəiflədə və sosial sabitliyi poza bilər [18]. Bu fenomen xüsusilə seçki prosesləri, ictimai qərarvermə və milli təhlükəsizlik məsələlərində ciddi risklər yaradır.

Transmilli rəqəmsal platformaların dominantlığı

Bu dominantlıq kiberməkanda yeni güc mərkəzlərinin formalaşmasına səbəb olmuşdur. Bu platformalar böyük həcmdə məlumatlara nəzarət etməklə yanaşı, informasiya axınlarının istiqamətini müəyyənləşdirmək imkanına malikdir. Nəticədə dövlətlərin normativ suverenliyi və informasiya siyasəti üzərində təsir imkanları məhdudlaşır [19].

Təhlükəsizlik və insan hüquqları arasında balansın qorunması

Kibertəhlükəsizlik siyasətinin həyata keçirilməsində ən mürəkkəb və həssas məsələlərdən biridir. Bir tərəfdən dövlətlər milli təhlükəsizliyi təmin etmək məqsədilə kiberməkan üzərində nəzarəti gücləndirməyə çalışır, digər tərəfdən isə bu tədbirlər söz azadlığı, şəxsi məlumatların qorunması və digər fundamental hüquqların məhdudlaşdırılması riskini yaradır [20]. Bu baxımdan balanslaşdırılmış və hüquqi baxımdan əsaslandırılmış yanaşmanın tətbiqi xüsusi əhəmiyyət kəsb edir. Bununla yanaşı, kiber cinayətkarlığın artması, süni intellekt əsaslı hücum texnologiyalarının inkişafı və kritik məlumatların sızması riskləri də müasir dövrdə kiberməkanın təhlükəsizlik arxitekturasını daha da mürəkkəbləşdirən amillər kimi çıxış edir. Bu çağırışlar dövlətlərin yalnız müdafiə mexanizmlərini deyil, həm də qabaqlayıcı və strateji idarəetmə yanaşmalarını inkişaf etdirməsini tələb edir.

V. AZƏRBAYCAN RESPUBLİKASINDA KİBERSUVERENLİK

Azərbaycan Respublikasında kibertəhlükəsizlik və kibersuverenliyin təmin olunması dövlət siyasətinin prioritet və strateji istiqamətlərindən biri kimi müəyyən edilmişdir [21]. Müasir dövrdə rəqəmsal transformasiya proseslərinin sürətlənməsi fonunda dövlətin informasiya təhlükəsizliyinin təmin edilməsi və milli kiberməkanın qorunması milli təhlükəsizlik sisteminin ayrılmaz tərkib hissəsinə çevrilmişdir. Rəqəmsal transformasiya proqramları çərçivəsində ölkədə elektron hökumət sistemlərinin genişləndirilməsi, dövlət xidmətlərinin rəqəmsallaşdırılması və informasiya-kommunikasiya texnologiyalarının tətbiqinin artırılması istiqamətində kompleks tədbirlər həyata keçirilir. Bu proseslər həm idarəetmənin effektivliyinin yüksəldilməsinə, həm də dövlət-vətəndaş münasibətlərində şəffaflığın və operativliyin təmin olunmasına xidmət edir. Eyni zamanda milli informasiya infrastrukturlarının – data mərkəzlərinin, dövlət informasiya sistemlərinin və kommunikasiya şəbəkələrinin təhlükəsizliyinin gücləndirilməsi istiqamətində sistemli yanaşma tətbiq olunur. Bu kontekstdə kibertəhlükəsizlik risklərinin idarə olunması, kritik informasiya infrastrukturlarının müdafiəsi və potensial kiberinsidentlərə qarşı operativ reaksiya mexanizmlərinin formalaşdırılması xüsusi əhəmiyyət kəsb edir. Azərbaycanın yerləşdiyi geosiyasi mühit və regionda müşahidə olunan informasiya qarşıdurmaları kibersuverenliyin təmin olunmasını daha da aktuallaşdırır. İnformasiya müharibəsi elementlərinin geniş tətbiqi, dezinformasiya kampaniyaları və kiberhücum riskləri dövlətin rəqəmsal təhlükəsizlik strategiyasının gücləndirilməsini zəruri edir [22]. Bu baxımdan kibersuverenliyin təmin olunması yalnız texniki və hüquqi tədbirlərlə məhdudlaşmır, eyni zamanda informasiya siyasətinin, strateji kommunikasiya mexanizmlərinin və milli rəqəmsal ekosistemin inkişafını da əhatə edir. Bundan əlavə, Azərbaycanın beynəlxalq kibertəhlükəsizlik təşəbbüslərində iştirakı, regional və qlobal əməkdaşlıq mexanizmlərinə inteqrasiyası ölkənin kibersuverenlik potensialının gücləndirilməsində mühüm rol oynayır. Bu əməkdaşlıq çərçivəsində təcrübə mübadiləsi, birgə təhlükəsizlik tədbirləri və normativ yanaşmaların uyğunlaşdırılması həyata keçirilir.

VI. HƏLL YOLLARI VƏ PERSPEKTİVLƏR

Kibersuverenliyin effektiv təmin olunması mürəkkəb və çoxsəviyyəli proses olmaqla, sistemli və inteqrasiya olunmuş yanaşmanın tətbiqini tələb edir. Müasir şəraitdə bu proses yalnız texnoloji vasitələrlə deyil, həm də hüquqi, institusional və strateji idarəetmə mexanizmləri vasitəsilə həyata keçirilməlidir. Bu kontekstdə aşağıdakı istiqamətlər xüsusi əhəmiyyət kəsb edir:

- Normativ-hüquqi bazanın təkmilləşdirilməsi – kiberməkanın hüquqi tənzimlənməsi sahəsində beynəlxalq standartlara uyğun milli qanunvericiliyin formalaşdırılması və tətbiqi mexanizmlərinin gücləndirilməsi [23]
- Texnoloji müstəqilliyin artırılması – yerli proqram təminatının, milli platformaların və informasiya sistemlərinin inkişaf etdirilməsi, xarici texnologiyalardan asılılığın azaldılması
- Elmi-tədqiqat fəaliyyətinin intensivləşdirilməsi – kibertəhlükəsizlik, süni intellekt və məlumat təhlükəsizliyi sahələrində fundamental və tətbiqi tədqiqatların genişləndirilməsi

- İnsan kapitalının inkişafı – ixtisaslı kadrların hazırlanması, peşəkar təlim proqramlarının təşkili və kibertəhlükəsizlik üzrə ekspert potensialının gücləndirilməsi
- Beynəlxalq və regional əməkdaşlığın genişləndirilməsi – kibertəhlükəsizlik sahəsində çoxtərəfli əməkdaşlıq mexanizmlərinin inkişaf etdirilməsi və qlobal təşəbbüslərdə aktiv iştirak

Bununla yanaşı, dövlətlər kibersuverenliyin təmin olunması istiqamətində preventiv və adaptiv yanaşmaları paralel şəkildə tətbiq etməlidir. Preventiv yanaşma risklərin əvvəlcədən müəyyənləşdirilməsinə və qarşısının alınmasına yönəldiyi halda, adaptiv yanaşma dəyişən kibertəhlükələrə operativ uyğunlaşma imkanlarını təmin edir.

Eyni zamanda rəqəmsal transformasiya strategiyalarının milli təhlükəsizlik prioritetləri ilə uzlaşdırılması kiberməkanda dayanıqlı idarəetmə modelinin formalaşdırılmasına şərait yaradır. Bu yanaşma dövlətin həm daxili sabitliyinin qorunmasına, həm də beynəlxalq rəqəmsal mühitdə rəqabət qabiliyyətinin artırılmasına xidmət edir.

Nəticə etibarilə, qeyd olunan tədbirlərin kompleks və sistemli şəkildə reallaşdırılması dövlətlərin kiberməkanda dayanıqlı mövqeyinin institusional əsaslarının möhkəmləndirilməsinə, rəqəmsal suverenliyin davamlı inkişafına və milli təhlükəsizlik sisteminin funksional effektivliyinin yüksəldilməsinə xidmət etməklə yanaşı, onların qlobal rəqəmsal nizam daxilində strateji mövqelərinin konsolidasiyasını və uzunmüddətli dayanıqlılığını təmin edən fundamental amil kimi çıxış edir [24].

NƏTİCƏ

Aparılan tədqiqat göstərir ki, kibersuverenlik müasir beynəlxalq münasibətlər sistemində dövlət suverenliyinin transformasiya olunmuş forması kimi çıxış edir və rəqəmsallaşma prosesləri dövlətlərin təhlükəsizlik yanaşmalarını yenidən formalaşdırmışdır. Müəyyən edilmişdir ki, kibersuverenlik yalnız texnoloji nəzarət mexanizmi deyil, həm də hüquqi və institusional çərçivədə dövlət müstəqilliyinin təmin olunmasının mühüm alətidir və dövlətlərin kiberməkanda strateji mövqeyini gücləndirir. Eyni zamanda, əsas çətinliklər beynəlxalq hüquqi fragmentasiya, texnoloji asılılıq və dezinformasiya kimi qeyri-ənənəvi təhdidlərlə bağlıdır ki, bu da dövlətlərin daha çevik və strateji idarəetmə yanaşmalarına keçidini zəruri edir. Azərbaycan Respublikası kontekstində kibersuverenlik milli təhlükəsizlik siyasətinin prioritet istiqaməti kimi çıxış edir və rəqəmsal transformasiya tədbirləri bu sahədə dayanıqlılığı gücləndirir. Nəticə olaraq, kibersuverenliyin effektiv təmin olunması hüquqi, texnoloji və institusional tədbirlərin inteqrasiya olunmuş şəkildə həyata keçirilməsini tələb edir və bu, dövlətlərin kiberməkanda dayanıqlı mövqeyinin və uzunmüddətli inkişafının əsas şərtidir.

ƏDƏBİYYAT

[1] J. S. Nye, Cyber Power. Cambridge, MA, USA: Harvard Kennedy School, 2010.
[2] L. DeNardis, The Global War for Internet Governance. New Haven, CT, USA: Yale University Press, 2014.
[3] M. Mueller, Will the Internet Fragment? Sovereignty, Globalization and Cyberspace. Cambridge, U.K.: Polity, 2017.
[4] T. Rid, Cyber War Will Not Take Place. Oxford, U.K.: Oxford University Press, 2013.
[5] United Nations, "Group of Governmental Experts (GGE) reports on developments in the field of information and telecommunications," 2021.
[6] M. N. Shaw, International Law. Cambridge, U.K.: Cambridge University Press, 2008.
[7] M. Schmitt, Ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, U.K.: Cambridge University Press, 2017.
[8] Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.
[9] European Union, "EU cybersecurity strategy for the digital decade," 2020.
[10] European Union Agency for Cybersecurity (ENISA), Cybersecurity Threat Landscape Report, 2022.
[11] Organisation for Economic Co-operation and Development (OECD), Digital Security Risk Management. Paris, France: OECD Publishing, 2015.
[12] M. Castells, The Rise of the Network Society. Oxford, U.K.: Wiley-Blackwell, 2010.
[13] J. A. Lewis, Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford, U.K.: Oxford University Press, 2018.
[14] S. J. Shackelford, Managing Cyber Attacks in International Law, Business, and Relations. Cambridge, U.K.: Cambridge University Press, 2014.
[15] D. B. Hollis, Cyber Operations and International Law. Oxford, U.K.: Oxford University Press, 2021.
[16] E. Morozov, The Net Delusion: The Dark Side of Internet Freedom. New York, NY, USA: PublicAffairs, 2011.
[17] Microsoft, Digital Defense Report, 2022.
[18] C. Wardle and H. Derakhshan, Information Disorder: Toward an Interdisciplinary Framework. Strasbourg, France: Council of Europe, 2017.
[19] S. Zuboff, The Age of Surveillance Capitalism. New York, NY, USA: PublicAffairs, 2019.
[20] United Nations, "Human rights in the digital age reports."
[21] Azerbaijan Republic, National Security Strategy, 2020.
[22] Various Authors, "Regional cybersecurity analytical reports."
[23] World Economic Forum, Global Cybersecurity Outlook, 2022.
[24] International Telecommunication Union (ITU), Global Cybersecurity Index.

The Concept of Cyber Sovereignty and Its Role in the State Security System

Ayna Alixanova

Museum of Azerbaijani literature named after Nizami Ganjavi, Baku, Azerbaijan

Abstract— The article analyzes the scientific and practical challenges of ensuring state cyber sovereignty. It substantiates that, in the context of modern digital transformation, cyberspace has become a new dimension of state sovereignty. The theoretical foundations of the concept of cyber sovereignty are examined, and its normative, technological, informational, and economic components are identified. Existing gaps in international law regarding the legal status of cyberspace, terminological ambiguities, technological dependence, and jurisdictional issues are evaluated from an academic perspective. At the same time, the practical challenges faced by states such as cyberattacks, disinformation, the dominance of transnational platforms, and the balance between security and human rights are analyzed. Within the context of the cybersecurity policy of the Republic of Azerbaijan, national priorities and prospective directions are determined. Ultimately, the strategic importance of cyber sovereignty as a key element of national security is substantiated.

Keywords— cyber sovereignty; cybersecurity; information security; digital transformation; cyber attack; disinformation; transnational platforms.