Dövlətin Kibersuverenliyinin Təmini üçün İnformasiya Qarşıdurması Strategiyalarının İşlənməsi

İradə Ələkbərova
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
airada.09@gmail.com

***Xülasə*— Tədqiqat işində müasir hibrid müharibələrin tərkib hissəsi olan informasiya qarşıdurması fonunda rəqəmsal dövlətin kibersuverenliyinin təmini məsələləri tədqiq olunur. Beynəlxalq təcrübə nəzərə alınaraq, kritik infrastrukturun kiberdayanıqlılığı və informasiya hücumlarının zəncirvari təsir mexanizmləri analiz edilir. Tədqiqat işində infrastruktur, informasiya, idarəetmə və hüquqi müstəviləri əhatə edən dörd mərhələli strateji model işlənib hazırlanmışdır. Tədqiqatın nəticələri rəqəmsal dövlətinsuverenliyini təkcə texniki müdafiə ilə deyil, həm də aktiv informasiya qarşıdurması strategiyaları və rəqəmsal etimadın qorunması ilə əlaqələndirir.**

Açar sözlər– kibersuverenlik; informasiya qarşıdurması; informasiya hücumu; infrastrukturun suverenliyi; kiberdayanıqlılıq.

I. GİRİŞ

İnformasiya qarşıdurması sosial-iqtisadi və siyasi maraqların toqquşması nəticəsində yaranan ziddiyyətlərin ən yüksək forması olub, qarşı tərəfin informasiya resurslarının məhvinə və ya nəzarətdə saxlanmasına yönələn informasiya əməliyyatlarıdır [1, 2]. İnformasiya qarşıdurması strategiyaları dedikdə, planlı şəkildə həyata keçirilən həm hücum, həm də müdafiə xarakterli rəqəmsal və sosiopsixoloji kompleks fəaliyyət planı nəzərdə tutulur. [3]. Bu baxımdan rəqəmsal texnologiyalar üzərindən dövlətin informasiya təhlükəsizliyinə və cəmiyyətin sabitliyinə təhdid yaradan informasiya müharibəsi, informasiya qarşıdurması və informasiya hücumu kimi informasiya əməliyyatlarına hazır olmaqla öz kibersuverenliyini təmin etmək hər bir dövlətin əsas strateji vəzifəsidir. Rəqəmsal dövlət kontekstində informasiya qarşıdurması strategiyalarının işlənməsi sadəcə texnoloji deyil, həm də milli təhlükəsizlik fəlsəfəsinin rəqəmsal formasıdır. Strategiyanın uğuru vətəndaşın rəqəmsal dövlətə olan inamının (digital trust) nə dərəcədə qorunmasından asılıdır.

Cəmiyyətin böyük hissəsinin cəlb olunması ilə baş verən yüksək intensivliyə malik informasiya qarşıdurmaları əksər hallarda ictimaiyyətə, dövlətə qarşı ciddi təhlükələrin yaranması ilə nəticələnir. İnformasiya qarşıdurmaları ictimai münasibətlərin strukturunu dəyişməklə informasiya müharibələri, kiber-hücumlar, hərbi münaqişələr də daxil olmaqla daha ağır fəsadlar yarada bilər.

İnformasiya hücumu və ya kiberhücum icazə olmadan istənilən şəkildə informasiyanın ələ keçirilməsi, məhv edilməsi və ya dəyişdirilməsinə, həmçinin, qarşı tərəfin proqram təminatlarına, gizli informasiyanın saxlandığı aparat təminatına və insan psixologiyasına yönəlmiş hücum əməliyyatlarıdır [4]. Kiberhücumlar müxtəlif dövlət xidmətləri, maliyyə əməliyyatları, sənaye və kosmik sistemlər kimi müxtəlif kritik infrastrukturlara ciddi təsir göstərə bilər [5].

Müvafiq olaraq, suveren dövlətlər bu təhdidlə mübarizə aparmaq üçün informasiya texnologiyalarının son nailiyyətlərindən, əsasən, süni intellekt (Sİ) texnologiyalarının tətbiqi ilə onlayn təhlükəsizlik və milli müdafiəni təmin edən müxtəlif proqramlar hazırlayırlar. İnformasiya texnologiyalarının inkişafı beynəlxalq münasibətlərdə və mübahisəli məsələlərdə güc tətbiqi anlayışını kökündən dəyişmişdir. Ənənəvi olaraq, BMT Nizamnaməsinin 2(4)-cü maddəsi dövlətlərin bir-birinin ərazi bütövlüyünə və ya siyasi müstəqilliyinə qarşı "güc tətbiq etməsini" qadağan edir [6].

İnformasiya müharibəsi özündə kiber-hücumu, informasiya müdafiəsi və informasiya qarşıdurması kimi əməliyyatları birləşdirən, həm dövlət, həm də cəmiyyət üçün ciddi təhlükə yaradan informasiya əməliyyatıdır [7]. İnformasiya müharibəsi qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi, hərbi potensialını ələ keçirmək, ictimai şüura təsir göstərməklə insanların davranışlarını dəyişmək və nəzarətdə saxlamaqla yanaşı öz kibersuverenliyini yüksək formada təmin etmək uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir.

Kibersuverenlik beynəlxalq münasibətlər, iqtisadi inkişaf, vətəndaşların rifahı, milli təhlükəsizlik məsələlərinin əsasını təşkil edir və kiber-məkanda qanunvericiliyin tətbiqini və milli maraqların təşviqini nəzərdə tutur [8]. Sİ, böyük verilənlər (big data) və hibrid təhdidlərin artması şəraitində dövlətin rəqəmsal sərhədlərini qorumaq, yəni kibersuverenliyi təmin etmək milli təhlükəsizliyin ən mühüm prioritetinə çevrilmişdir. Milli rəqəmsal ekosistemlərin qorunması üçün effektiv kibertəhlükəsizlik və informasdiya qarşıdurması strategiyalarının necə qurulmalı olduğu məsələsi bu gün əsas tədqiqat obyektlərindəndir [9].

Xarici kiber-müdaxilələr və dezinformasiya kampaniyaları qarşısında yalnız müdafiə xarakterli deyil, həm də proaktiv informasiya qarşıdurması strategiyalarının işlənilməsi bu mövzunu strateji əhəmiyyətli və aktual edir. Tədqiqatın məqsədi müasir informasiya müharibələri təhdidlərini analiz etməklə dövlətin rəqəmsal müstəqilliyini, yəni kibersuverenliyini qorumağa imkan verən, daxili və xarici kiber-təhdidlərə qarşı dayanıqlı informasiya qarşıdurması strategiyalarını və onların tətbiqi modelini işləyib hazırlamaqdır. Tədqiqatın obyekti müasir informasiya qarşıdurmaları şəraitində dövlətin milli informasiya məkanı, kritik informasiya infrastrukturu və dövlət idarəçiliyinin

DOI: 10.25045/cyber.gov.2026.14

rəqəmsal seqmentləridir. Tədqiqatın predmeti isə, informasiya müharibəsi texnologiyalarına qarşı kibersuverenliyin təmini mexanizmləri və effektiv informasiya qarşıdurması strategiyalarının formalaşdırılması prinsipləridir.

II. ƏLAQƏLİ İŞLƏR

Dövlət suverenliyinin kiberməkanda rolu akademik ədəbiyyatlarda geniş müzakirə olunmaqdadır. Bu müzakirələrdə əsasən kibersuverenliyə olan təhdidlər, onlarla mübarizə metodları, beynəlxalq hüquq prinsiplərinin kiberməkanda necə tətbiq oluna biləcəyi və bu kontekstlərdə mövcud problemlərin həlli kimi məsələlərə baxılır. Milli rəqəmsal ekosistemlərin qorunması üçün effektiv kibertəhlükəsizlik strategiyalarının necə qurulmalı olduğu məsələsi bu gün əsas tədqiqat obyektlərindəndir [10].

Kiber-təhdidlərin idarə edilməsi və texnoloji infrastrukturun qorunmasına həsr olunan BMT-nin Baş İcraçı Direktorlar Şurasının (Chief Executives Board, CEB) kibertəhlükəsizlik və kibercinayətkarlıqla bağlı rəsmi sənədində kibersuverenlik – texnoloji muxtariyyət, daxili koordinasiya imkanları və kibertəhdidlərin müstəqil qiymətləndirilməsi mexanizmlərinin vəhdəti kimi qəbul edilir [11].

Kibersuverenliklə əlaqədar aparılan tədqiqatlar, əsasən, onun siyasi və hərbi aspektlərinə diqqət yetirir. Kibersuverenliyin ilkin tədqiqatlarında daha çox verilənlərin suverenliyi, texnoloji suverenlik və mülkiyyət hüququ problemləri araşdırılır [12]. Bəzi tədqiqatçılar kibersuverenliyi dövlətin kiberhücumlara qarşı özünü müdafiə etmə qabiliyyəti kimi təsvir edir [13]. Belə tədqiqatlarda kibersuverenlik kritik infrastrukturun qorunması baxımından, daha çox milli təhlükəsizlik və xarici təhdidlərdən müdafiə kontekstində təhlil edilir, dövlətlərin texnoloji, qanunverici və insan resursları suverenliyini gücləndirmək üçün atdığı addımlar (məsələn, milli bulud xidmətlərinin genişləndirilməsi, kibertəhlükəsizlik məsələlərində Sİ texnologiyalarından geniş istifadə və s.) araşdırılır.

Kibersuverenliklə bağlı tədqiqatlarda həmçinin bəzi dövlətlərin internet resursları üzərində həyata keçirməyə çalışdığı nəzarət və dövlət suverenliyi prinsiplərinə əsaslanan senzura üçün hüquqi əsaslandırmalar təhlil edilir. Məsələn, Niderland və Avropa İttifaqı tərəfindən hazırlananan kibersuverenlik və strateji muxtariyyət məsələlərini təhlil edən hesabatda [14], kibersuverenliyin təminində kibertəhlükəsizlik konsepsiyası ən yüksək siyasi prioritet kimi qəbul edilir. Müəlliflər iddia edirlər ki, kibersuverenliyə nail olmaq üçün beynəlxalq tərəfdaşlıqların qurulması və investisiya, tənzimləmə və innovasiya siyasətlərinin birləşdirilməsi vacibdir. Xüsusilə bulud sistemləri, 6G, kriptoqrafiya, Sİ və kvant texnologiyaları sahələrində hədəfəyönlü fəaliyyətlər tələb olunur.

BMT-nin Terrorizmlə Mübarizə İdarəsi (UNOCT) tərəfindən həyata keçirilən "Kibertəhlükəsizlik və yeni texnologiyalar" (Cybersecurity and New Technologies) proqramı, müasir dövrün ən mürəkkəb təhlükəsizlik çağırışlarından birinə – rəqəmsal texnologiyaların terror məqsədi üçün istifadəsinə qarşı yönəlmişdir[15]. Proqramın əsas hədəfi üzv dövlətlərin və özəl təşkilatların kritik infrastrukturunun (enerji şəbəkələri, su təchizatı, nəqliyyat, maliyyə sistemləri) terrorçuların kiberhücumlarından qorumaq potensialını artırmaqdır. Burada söhbət təkcə müdafiədən deyil, həm də terrorçuların yeni texnologiyalardan istifadə edərək həyata keçirdikləri fəaliyyətlərin qarşısının əvvəlcədən alınmasından gedir.

BMT-nin Regionalararası Cinayət və Ədalət Araşdırmaları İnstitutunun (United Nations Interregional Crime and Justice Research Institute, UNICRI) strategiyasına həsr olunmuş sənəddə "Rəqəmsal Suverenlik" və "Hüquqi Suverenlik" konsepsiyaları mərkəzi yer tutur [16]. Sənəddə hər bir dövlətin suverenliyinin onun həyati əhəmiyyətli sistemlərinin (enerji, su, rabitə) xarici kibermüdaxilələrdən qorunmasından asılı olduğu bildirilir. Bu yanaşmada kibersuverenlik iki tərəfli təsvir edilir: müdafiə (texnologiyanın cinayət alətinə çevrilməsinin qarşısını almaq) və hücum/nəzarət (hüquq-mühafizə orqanlarının “data mining” və onlayn profil vasitəsilə suverenliyi bərpa etməsi).

Kibersuverenlik akademik ədəbiyyatda və beynəlxalq təşkilatlarda ətraflı müzakirə olunsa da, rəqəmsal dövlət sektoruna yönəlmiş kiber-hücumların digər strateji sahələrə kaskad təsirləri və vahid fəaliyyət hədəfləri hələ də tam sistemləşdirilməmişdir. Xüsusilə, Sİ texnologiyalarının sürətli inkişafı fonunda kibersuverenliyin təmini çərçivəsində informasiya qarşıdurması strategiyalarının yenidən işlənməsinə ehtiyac vardır.

III. İNFORMASİYA QARŞIDURMASI STRATEGİYALARI

İnformasiya qarşıdurması strategiyalarının müəyyən edilməsi və analizi həm hərbi-strateji, həm də texnoloji yanaşmaların sintezini tələb edir. Bu proses, rəqibin niyyətini anlamaqdan başlayaraq, hücumun miqyasını proqnozlaşdırmağa qədər bir neçə mərhələdən ibarətdir. İnformasiya qarşıdurması strategiyalarının müəyyən edilməsi rəqəmsal dövlətin zəif nöqtələrinin və rəqibin resurslarının qiymətləndirilməsinə əsaslanır. Rəqibin resurslarının qiymətləndirilməsi üçün onun informasiya qarşıdurmasında tətbiq etdiyi strategiyaların analizi, hücuma cavab olaraq hədəf və vasitələrin düzgün seçilməsi əsas məsələlərdəndir:

- İnformasiya qarşıdurması strategiyalarının analizi. Bu proses qarşı tərəfdən yönəlmiş informasiya hücumun hansı metodla və hansı məqsədlə edildiyini üzə çıxarmağa xidmət edir.
- Hədəfinin müəyyən olunması. Bu hədəflərə ictimai rəy, kritik infrastruktur və ya qərar qəbulu mexanizmləri aid ola bilər.
- İstifadə olunacaq vasitələrin müəyyən olunması. Bu mərhələdə bot şəbəkələri, dezinformasiya kanalları və kiber-alətlər seçilir.
- Zamanlamanın (Timing) düzgün seçilməsi. İnformasiya əməliyyatının ən həssas məqamda başlanması nəzərdə tutulur. Məsələn, informasiya qarşıdurmaları əksər hallarda seçkilər, iqtisadi böhran, sosial gərginlik və ya hərbi münaqişə zamanı həyata keçirilir.

Rəqəmsal transformasiya şəraitində dövlətin suverenliyi yalnız coğrafi sərhədlərin qorunması ilə deyil, həm də milli kritik infrastrukturun kiberdayanıqlılığı ilə ölçülür. Bu infrastrukturun mərkəzində isə SCADA (Supervisory Control and Data Acquisition) sistemləri dayanır. Enerji şəbəkələri, su təchizatı, nəqliyyat və hərbi logistika kimi həyati əhəmiyyətli sahələrin idarə edilməsi bu sistemlərin fasiləsiz və təhlükəsiz işləməsindən asılıdır. İnformasiya qarşıdurması strategiyasına rəqəmsal dövlət (e-government) kontekstindən yanaşdıqda, əsas fokus, məlumatların bütövlüyü, idarəetmənin kiberdayanıqlılığı və vətəndaş-dövlət münasibətlərinin rəqəmsal suverenliyi üzərinə düşür. Bu strategiyanın işlənməsini 4 əsas konseptual mərhələdə həyata keçirmək olar:

1) Rəqəmsal infrastrukturun suverenliyi (Server səviyyəsində). Strategiyanın təməli dövlətin rəqəmsal xidmətlərinin kənar təsirlərdən asılılığını minimuma endirməkdir. Bunun üçün milli bulud strategiyasının işlənməsi vacibdir. Nəticədə bütün dövlət məlumatlarının və reyestrlərinin vahid, qapalı və milli nəzarətdə olan serverlərdə cəmləşməsi əldə oluncaqdır.

2) İnformasiya qarşıdurmasında "Rəqəmsal qalxan" modeli (İnformasiya səviyyəsində) [17]. Dövlət xidmətləri haqqında yayılan saxta xəbərləri (məsələn, bank sisteminin çökməsi xəbəri) real vaxt rejimində rəsmi rəqəmsal platformalar vasitəsilə təkzib edən mexanizmlərin qurulması vacibdir. Həmçinin, vətəndaşların fərdi məlumatlarının sızmasının (data breach) qarşısının alınması strategiyanın ən vacib hissəsidir. Belə ki, bu sızıntılar dövlətə qarşı rəqəmsal etimadı azaltmağa yönəlmişdir.

3) İdarəetmənin adaptivliyi və müdafiə (İdarəetmə səviyyəsində). İnformasiya qarşıdurması strategiyası informasiya hücumu zamanı rəqəmsal dövlətin çevik qərar verməsini təmin etməlidir.

4) Kibersuverenliyin beynəlxalq hüquqi təsdiqi və rəqəmsal etika (Hüquqi səviyyə). Strategiyanın yekun mərhələsi daxili kiber-müdafiə sisteminin beynəlxalq normalarla uzlaşdırılması və rəqəmsal cəmiyyətin dayanıqlılığının etik təməllər üzərində qurulmasıdır. Bir dövlət tərəfindən həyata keçirilən kiberhücum digər dövlətin kritik infrastrukturuna (su, elektrik, səhiyyə) kinetik effektlə eyni dərəcədə zərər vurursa, BMT Nizamnaməsinin 51-ci maddəsinə əsasən [18] həmin dövlətin hərbi (kinetik) cavab vermə hüququ yaranır. Bu, qlobal sabitlik üçün böyük riskdir və gərginliyin kinetik müharibəyə keçməməsi üçün şəffaflıq və beynəlxalq əməkdaşlıq kanallarının qurulması vacibdir.

Cədvəl 1-də təqdim olunan informasiya qarşıdurması strategiyaları cədvəli rəqəmsal dövlətin kibersuverenliyini aktiv, adaptiv və hüquqi əsaslı idarəetməyə transformasiya edir. Bu sistemin tətbiqi, dövlətin rəqəmsal sərhədlərini fiziki sərhədlər qədər toxunulmaz edir və hibrid müharibələr şəraitində milli təhlükəsizliyin texnoloji suverenliyini təmin edir. Cədvəldən göründüyü kimi, rəqəmsal dövlətdə kibersuverenliyin təmini üçün informasiya qarşıdurması strategiyaları dövlətin kiberdayanıqlılığını (R) təmin edir.

İnformasiya qarşıdurması çərçivəsində kiberdayanıqlılıq modeli dövlətin rəqəmsal sərhədlərini fiziki sərhədlər qədər toxunulmaz edir:

$$R = \int_0^t (\alpha \cdot S_{\text{inf}} + \beta \cdot S_{shield} + \gamma \cdot A_{adapt} + \delta \cdot L_{legit}) \cdot dt$$

$$(1)\ \alpha, \beta, \gamma, \delta \in [0,1]$$

CƏDVƏL 1. RƏQƏMSAL DÖVLƏTDƏ KİBERSUVERENLİYİN TƏMİNİ ÜÇÜN İNFORMASİYA QARŞIDURMASI STRATEGİYALARI

Strateji mərhələ	Texnologiya	Strateji məqsəd
1. İnfrastruktur suverenliyi	Milli server/bulud, kvant şifrələmə	Xarici texnoloji asılılığın aradan qaldırılması və risklərin neytrallaşdırılması.
2. Rəqəmsal qalxan modeli	Təbii dilin emalı, Sentiment analiz	Dezinformasiya və fake xəbərlərə qarşı avtomatik təkzib; vətəndaşın rəqəmsal etimadının qorunması.
3. Adaptiv idarəetmə və müdafiə	AI-SOC, maşın təlimi, dərin təlim	Hücum mənbəyinin təyini; "Məlumat zəhərləməsi" ilə rəqibin alqoritmlərinin sıradan çıxarılması.
4. Kibersuveren-liyin təsdiqi	Rəqəmsal sübut bazası, Beynəlxalq kiber-diplomatiya	Kiber-təcavüzün dövlət sərhədinə hücum kimi tanınması; beynəlxalq sübut bazasının yaradılması.

S_{inf} – kritik infrastrukturun texnoloji suverenliyidir (milli bulud və server). Əgər kritik infrastruktur (məsələn, SCADA) xarici proqram təminatından 100% asılıdırsa, dayanıqlılıq sıfıra enir. Bu komponent milli serverlərin, kvant şifrələmənin və yerli kontrollerlərin mövcudluğunu təmsil edir.

S_{shield} – "Rəqəmsal qalxan" modelidir, yəni informasiya məkanının manipulyasiyalardan qorunma səviyyəsidir. maşın təlimi (MT) metodları vasitəsilə dezinformasiyaya qarşı avtomatik təkzib mexanizmini ifadə edir. Sülh dövründə β minimaldır, sistem yalnız monitorinq aparır. Fövqəladə hal və ya informasiya qarşıdurması yaranarsa β maksimum qiymət alır və nəticədə "rəqəmsal qalxan" resursların əsas hissəsini cəmiyyətin psixoloji dayanıqlılığını qorumağa yönəldir.

A_{adapt} – sistemin hücumlara qarşı adaptasiya qabiliyyətidir (Sİ əsaslı analiz, proqnozlaşdırıcı analitika və və aktiv müdafiə qabiliyyəti). Burada əsas iş AI-SOC (Security Operations Center) sisteminin üzərinə düşür. AI-SOC suni intellekt alqoritmləri vasitəsilə kiber-hücumları hələ baş vermədən proqnozlaşdırır və avtonom şəkildə dəf edən, rəqəmsal dövlətin kibersuverenliyini qoruyan avtomatlaşdırılmış "immunitet sistemi"dir. Bu sistem olmadan müasir hibrid müharibələrin yüksək sürətli kiber-hücumlarına qarşı effektiv müdafiə qurmaq qeyri-mümkündür.

L_{legit} – kibersuverenliyi təsdiq edən hüquqi bazadır. Dövlətin kiber-hücuma qarşı beynəlxalq hüquq müstəvisində cavab vermə qabiliyyətidir və dövlətin müxtəlif hüquqi resurslarının vəhdətini ifadə edir. Bu resurslara aiddir:

- Rəqəmsal sübut bazası. Kiber-hücumun izlərinin beynəlxalq məhkəmələrdə qəbul edilə bilən formatda sənədləşdirilməsi.
- Kiber-diplomatiya. İkitərəfli və çoxtərəfli müqavilələr vasitəsilə qarşı tərəfin apardığı informasiya-hücumlarının beynəlxalq səviyyədə pislənməsinə və sanksiyaların tətbiqinə nail olmaq.

- Milli qanunvericilik. Kiber-məkanın dövlət sərhədi kimi tanınması və bu məkandakı hər hansı müdaxiləni dövlət suverenliyinin pozulması kimi rəsmiləşdirməsi.

α, β, γ, δ – çəki əmsallarıdır və MT vasitəsilə təhdid mühitinə uyğun olaraq dinamik tənzimlənr. Bu əmsallar dövlətin prioritetini göstərir. Məsələn, aktiv müharibə şəraitində dövlət adaptiv müdafiəyə (β) daha çox çəki verə bilər, sülh dövründə isə infrastruktura (α) daha çox çəki verilə bilər. Dayanıqlılıq (*R*) zaman keçdikcə sistemin öyrənmə qabiliyyəti (Sİ vasitəsilə) sayəsində artmalıdır. Əgər inteqralın nəticəsi zamanla böyüyürsə, deməli, dövlət hər bir hücumdan dərs çıxararaq daha güclü "rəqəmsal immunitet" qazanır. Dövlətin kiberdayanıqlılığı infrastruktur suverenliyi, adaptiv müdafiə və hüquqi legitimlik komponentlərinin zaman daxilindəki kəsilməz inteqrasiyasından asılı olan dinamik bir prosesdir.

NƏTİCƏ

Tədqiqat göstərir ki, müasir dövrdə dövlətin suverenliyi artıq yalnız onun fiziki sərhədləri ilə deyil, həm də rəqəmsal məkan üzərindəki nəzarəti və kiberdayanıqlılığı ilə ölçülür. Rəqəmsal dövlət infrastrukturunun sektorları (enerji, maliyyə, rabitə, səhiyyə və s.) bir-birindən asılı sinir sistemi kimi fəaliyyət göstərir və bir sektordakı zəiflik domino effekti ilə bütün dövlət idarəçiliyini iflic edə bilər. Tədqiqatdan o da məlum oldu ki, informasiya qarşıdurmasında üstünlük əldə etmək və kibersuverenliyi təmin etmək üçün ənənəvi müdafiə üsulları kifayət deyil. MT və Sİ əsaslı proqnozlaşdırıcı analitika vasitəsilə hücumun mənbəyini və tipini real vaxt rejimində təyin etmək vacibdir. "Rəqəmsal qalxan", AI-SOC və kiberdayanıqlılıq kimi modellər vətəndaş-dövlət etimadını qorumaq və informasiya qarşıdurmasında üstünlük əldə etmək üçün avtomatik təkzib mexanizmləri təklif edir. Dünyada informasiya qarşıdurmalarının və hərbi münaqişələrin artdığı bir şəraitdə hər bir dövlətin kibersuverenliyinin təmini beynəlxalq hüquqi bazaya söykənməlidir. Kiber-təcavüzün dövlət sərhədinə hücum kimi tanınması dövlətin özünümüdafiə hüququnu legitim edir. Təklif edilən 4 mərhələli informasiya qarşıdurması strategiyası rəqəmsal dövləti xarici texnoloji asılılıqdan və kiber-təhdidlərdən qoruyan universal bir modeldir. Bu modelin tətbiqi hibrid müharibələr əsrində dövlətin informasiya təhlükəsizliyini və rəqəmsal suverenliyini təmin edən ən effektiv həll yollarından hesab edilə bilər.

ƏDƏBİYYAT

[1] Straub, J., (2019), Mutual Assured Destruction in Information, Influence and Cyber Warfare: Comparing, Contrasting and Combining Relevant Scenarios, Technology in Society, pp. 101177, 2019.

[2] J. Straub, "Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios," Technology in Society, p. 101177, 2019.

[3] S. N. Bukharin and V. V. Tsyganov, Methods and Technologies of Information Wars. Moscow, Russia: Academic Project, 2007

[4] D. A. Gubanov, D. A. Novikov, and A. G. Chkhartishvili, Social Networks: Models of Information Influence, Control and Confrontation. Moscow, Russia: Publishing House of Physical and Mathematical Literature, 2010.

[5] U. Pagallo, "Cyber force and the role of sovereign states in informational warfare," Philosophy & Technology, vol. 28, no. 3, pp. 407–425, 2015. [Online]. Available: https://link.springer.com/article/10.1007/s13347-014-0177-4

[6] T. Ruys, "The meaning of 'force' and the boundaries of the jus ad bellum: Are 'minimal' uses of force excluded from UN Charter Article 2(4)?," American Journal of International Law, vol. 108, no. 2, pp. 159–210, 2014.

[7] G. Lilienthal and N. Ahmad, "Cyber-attack as inevitable kinetic war," Computer Law & Security Review, vol. 31, no. 3, pp. 390–400, 2015, doi: 10.1016/j.clsr.2015.03.002.

[8] A. Shoker, "Digital sovereignty strategies for every nation," Applied Cybersecurity & Internet Governance, vol. 1, no. 1, pp. 1–17, 2022, doi: 10.5604/01.3001.0016.0943.

[9] I. K. Kwentoa, "Cybersecurity in digital sovereignty: Protecting national digital ecosystems against foreign cyber infiltration in the age of decentralized technology," Journal of Next-Generation Research 5.0, 2025, doi: 10.70792/jngr5.0.v1i4.130.

[10] S. Couture and S. Toupin, "What does the concept of 'sovereignty' mean in digital, network and technological sovereignty?," SSRN Electronic Journal, vol. 21, no. 10, pp. 2305–2322, 2018, doi: 10.2139/ssrn.3107272.

[11] UN System Chief Executives Board for Coordination (CEB), "Cybersecurity," 2018. [Online]. Available: https://unsceb.org/topics/cybersecurity

[12] Y. Shen, "Cyber sovereignty and the governance of global cyberspace," Chinese Political Science Review, vol. 1, no. 1, pp. 81–93, 2016.

[13] N. Akhtar and A. R. Iqbal, "Cyber sovereignty: National security in the digital age," Lahore Institute for Research and Analysis Journal, vol. 3, pp. 87–104, 2025.

[14] P. Timmers, M. Punter, and C. Stolwijk, "Cybersecurity and digital sovereignty – Bridging the gaps," 2024. [Online]. Available: https://publications.tno.nl/publication/34643188/DvSKsfCM/timmers-2024-cybersecurity.pdf

[15] UN Counter-Terrorism Centre (CTC), "Cybersecurity and new technologies," 2020. [Online]. Available: https://www.un.org/counterterrorism/en/cybersecurity

[16] United Nations Interregional Crime and Justice Research Institute (UNICRI), "United Nations convention against cybercrime," 2024. [Online]. Available: https://www.unodc.org/unodc/en/cybercrime/convention/home.html

[17] M. A. Demir, "Digital shield: The protective role against human rights violations in cyber interventions," Cyberpolitik Journal, vol. 10, no. 20, pp. 112–134, 2025.

[18] United Nations, "Charter of the United Nations," 2016. [Online]. Available: https://legal.un.org/repertory/art51.shtml

Development of Information Conflict Strategies to Ensure the State's Cyber Sovereignty

Irada Alakbarova

Institute of Information Technology, Baku, Azerbaijan

Abstract— The research study examines the issues of ensuring the cyber sovereignty of the digital state against the background of information conflict, which is an integral part of modern hybrid wars. Taking into account international experience, the cyber resilience of critical infrastructure and the chain reaction mechanisms of information attacks are analyzed. The research study developed a four-stage strategic model covering the infrastructure, information, management, and legal levels. The results of the study link the sovereignty of the digital state not only with technical defense but also with active information conflict strategies and the preservation of digital trust.

Keywords— cyber sovereignty; information conflict; information attack; infrastructure sovereignty; cyber resilience.