Dövlətin Kiberimmunitetinin Yüksəldilməsi Yollarının Araşdırılması

Ramiz Şıxəliyev
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shikhramiz61@gmail.com

Xülasə— Bu gün informasiya-kommunikasiya texnologiyaları (İKT) dövlətlərin idarəetmə, iqtisadi, sosial və təhlükəsizlik sistemlərində geniş istifadə edilir. İKT-nin sürətli inkişafı yeni mürəkkəb, çoxvektorlu və süni intellekt əsaslı kiberhücumların yaranmasına gətirib çıxarmışdır. Ənənəvi reaktiv müdafiə modelləri bu kiberhücumlara qarşı o qədər də effektiv deyil. Buna görə, kiberimmunitet dövlət informasiya sistemlərinin adaptiv, proaktiv və özü öyrənən mexanizmlərlə kibertəhlükəsizliyini təmin edən strateji yanaşma kimi aktuallaşır. Bioloji immun sistemin prinsiplərinə əsaslanaraq, dövlət kiberimmuniteti erkən aşkarlama, adaptiv reaksiya, immun yaddaş və öz-özünü bərpa imkanlarını birləşdirərək milli kibersuverenliyin təmin edilməsinə imkan verər. Məqalədə mövcud kibertəhdidlərin xüsusiyyətləri və ənənəvi reaktiv kibertəhlükəsizlik yanaşmalarının məhdudiyyətləri analiz edilir və dövlətin kiberimmunitetnin yüksəldilməsi yolları araşdırılır.

Açar sözlər— kiberimmunitet; kibertəhlükəsizlik; kibersuverenlik; kiberdayanıqlılıq; adaptiv müdafiə; bio-əsaslı kibermüdafiə.

I. GİRİŞ

Müasir dövrdə informasiya-kommunikasiya texnologiyaları dövlətlərin fəaliyyətinin bütün sahələrinə nüfuz etmiş və onların idarəetmə, iqtisadi, sosial və təhlükəsizlik sistemlərinin əsas infrastruktur elementinə çevrilmişdir. Elektron hökumət platformalarının tətbiqi, rəqəmsal iqtisadiyyatın sürətli inkişafı, kritik infrastruktur obyektlərinin avtomatlaşdırılması, eləcə də bulud, mobil və paylanmış hesablama texnologiyalarının geniş yayılması dövlətlərin fəaliyyətini daha çevik, operativ və səmərəli etmişdir [1]. Lakin bununla yanaşı, dövlətlər üçün yeni kiberrisklər yaranmış və kibertəhdidlər artmışdır. Nəticədə, kibertəhlükəsizlik milli təhlükəsizliyin, dövlət suverenliyinin və iqtisadi dayanıqlılığın əsas komponentlərindən birinə çevrilmişdir [2].

Adətən, dövlətlərə qarşı kibertəhdidlər coğrafi sərhədlərlə məhdudlaşmır və qlobal xarakter daşıyır [3]. Lakin bu kibertəhdidlərə qarşı həyata keçirilən kibertəhlükəsizlik tədbirləri əsasən milli səviyyədə formalaşdırılır və bir çox hallarda onların qarşısını adekvat şəkildə almaq üçün kifayət etmir. Bununla yanaşı, tətbiq olunan ənənəvi kibertəhlükəsizlik modelləri əsasən reaktiv xarakter daşıyır və hücum və ya pozuntu baş verdikdən sonra müdafiə mexanizmlərinin işə düşməsinə əsaslanır [4]. Belə yanaşma dinamik və sürətlə dəyişən müasir kibertəhdid mühitində o qədər də effektiv deyil.

Müasir kiberhücumlar daha mürəkkəb, çoxvektorlu və uzunmüddətli xarakter daşıyır. Onların avtomatlaşdırması və ənənəvi müdafiə mexanizmlərindən yayınması üçün süni intellekt və maşın təlimindən istifadə olunur [5]. Bununla yanaşı, kibertəhdid mənbələri artıq ayrı-ayrı haker qrupları ilə məhdudlaşmır, həmçinin dövlət dəstəyi ilə həyata keçirilən kiberhücumları, kiberterrorizm şəbəkələrini, hibrid müharibə elementlərini, informasiya-psixoloji təsir mexanizmlərini, süni intellekt əsaslı hücum alqoritmlərini və sıfırıncı-gün hücum mexanizmlərini istifadə edən zərərli proqramları əhatə edir [1].

Belə mürəkkəb kiberhücum mühitində yalnız ənənəvi mühafizə mexanizmləri vasitəsitələri ilə dövlətin kibertəhlükəsizliyini effektiv şəkildə təmin etmək mümkün deyil. Bu səbəbdən proaktiv, adaptiv və öz-özünü öyrənən müasir kibertəhlükəsizlik sistemlərinin yaradılması məsələsi aktuallaşır [6]. Bu zaman kibertəhlükəsizlik sistemi ayrıca texniki mühafizə vasitəsi kimi deyil, dövlətin ümumi rəqəmsal arxitekturasına inteqrasiya olunmuş kompleks və adaptiv mexanizm kimi formalaşdırılmalıdır. Belə bir müdafiə arxitekturasının yaradılması üçün kiberimmunitet anlayışının istifadəsi xüsusi əhəmiyyət kəsb edir [7].

Kiberimmunitet bioloji immun sisteminin prinsiplərinə əsaslanır və erkən aşkarlama, adaptiv reaksiya, immun yaddaş, kollektiv müdafiə və öz-özünü bərpa kimi xüsusiyyətləri özündə birləşdirir [5]. Bu prinsiplər əsasında dövlət səviyyəsində proaktiv, öz-özünü öyrənən və real vaxt rejimində adaptasiya imkanına malik milli kiberimmun sisteminin yaradılması mühüm strateji məsələdir [8]. Kiberimmunitet süni intellektə əsaslanan hücumlar da daxil olmaqla, yeni nəsil təhdidlərə qarşı mühafizə təmin edə bilər [6].

Məqalənin məqsədi dövlətin üzləşdiyi müasir kibertəhdidlərin xüsusiyyətlərini və ənənəvi reaktiv kibertəhlükəsizlik yanaşmalarının məhdudiyyətlərini analiz edilməsi, həmçinin bioloji immun sistemlərinin prinsiplərinə əsaslanan kiberimmunitet konsepsiyası çərçivəsində dövlətin kiberdayanıqlılığının yüksəldilməsi yollarını araşdırılmasıdır.

II. DÖVLƏTİN KİBERTƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİNİN MÖVCUD YANAŞMALARI VƏ KONSEPTUAL ƏSASLARI

A. Milli kibertəhlükəsizliyə mövcud yanaşmalar

Son iki onillikdə dövlətlər kibertəhlükəsizliyin təmin edilməsi üçün milli strategiyalar, hüquqi çərçivələr və institusional strukturlara əsaslanan müxtəlif yanaşmalar işləmişlər [9]. Bu yanaşmalar kritik informasiya infrastrukturlarının müdafiəsinə, məlumatların məxfiliyinin, bütövlüyünün və əlçatanlığının təmin edilməsinə və vacib

DOI: 10.25045/cyber.gov.2026.07

xidmətlərin dayanıqlılığının təmin edilməsinə yönəlmiş texniki və təşkilati tədbirləri birləşdirir [10].

İlk milli kibertəhlükəsizlik modelləri əsasən müdafiə və reaktiv xarakter daşıyırdı və hökumət informasiya sistemlərinin mühafizəsinə və insidentlərə cavab qruplarının yaradılmasına yönəlmişdi [11]. Lakin zaman keçdikcə milli kibertəhlükəsizliyin əhatə dairəsi xeyli genişlənmişdir və müasir strategiyalar artıq risklərin idarə edilməsi, təhdid kəşfiyyatı, dövlət-özəl tərəfdaşlığı, potensialın yüksəldilməsi, kiber diplomatiya və dayanıqlılıq planlaşdırması kimi elementləri özündə birləşdirir [12]. Müasir yanaşmalar həmçinin "bütün hökumət" və "bütün cəmiyyət" modellərini əhatə edir. Bu çərçivələr enerji, maliyyə, səhiyyə, nəqliyyat və telekommunikasiya kimi vacib infrastrukturların özəl qurumlar tərəfindən idarə olunmasını və dövlət, sənaye və vətəndaş cəmiyyəti arasında əlaqələndirilmənin vacibliyini qəbul edir [11]. Nəticədə, milli kibertəhlükəsizlik siyasətləri təcrid olunmuş texniki müdafiədən daha çox əməkdaşlığa, məlumat mübadiləsinə və risklərin kollektiv idarə edilməsinə yönəlir [13].

B. Kibermüdafiə, kiberdayanıqlılıq və kiberimmunitet konsepsiyaları

Milli kibertəhlükəsizliyin məqsədlərini və mexanizmlərini təsvir etmək üçün bir neçə konseptual çərçivə mövcuddur. Bunların arasında kibermüdafiə, kiberdayanıqlılıq və kiberimmunitet konsepsiyaları mühüm əhəmiyyət kəsb edir.

Kibermüdafiə ənənəvi olaraq kiber təhdidlərin aşkar edilməsi, qarşısının alınması və onlara cavab verilməsi üçün nəzərdə tutulmuş texniki və təşkilati tədbirlər toplusunu əhatə edir [4]. Kibermüdafiə müdaxilələrin aşkarlanması sistemləri, insidentlərə cavab verilməsi və zərərli fəaliyyətlərin azaldılmasına yönəlmişdir. Bu konsepsiya kiberhücumların qarşının alınması və müdafiə vasitələri əsasında kibertəhlükəsizliyin təmin edilməsini nəzərdə tutur [14].

Kiberdayanıqlılıq yalnız kiberhücumların qarşısının alınması deyil, həmçinin sistemlərin, təşkilatların və cəmiyyətlərin kiberhücumları qabaqcadan görmək, onlara tab gətirmək və onlara uyğunlaşmaq qabiliyyətidir [15]. Bu konsepsiya mürəkkəb rəqəmsal mühitlərdə kiberhücumların tam qarşısının alınmasının qeyri-real olduğunu qəbul edir və buna görə də diqqət əsasən əməliyyatların davamlılığına, sürətli bərpaya və adaptiv öyrənməyə yönəlir [16].

Kiberimmunitet bioloji immun mexanizmlərinə əsaslanan daha yeni və inkişaf etməkdə olan bir konsepsiyadır [6]. O, kibertəhlükəsizliyi sistemlərin anomaliyaları müstəqil şəkildə aşkarlama, keçmiş hücumlardan dərs çıxarma və daimi xarici müdaxilə olmadan qoruyucu mexanizmləri inkişaf etdirmək imkanına malik dinamik, özünü tənzimləyən və adaptiv bir proses kimi formalaşdırır [5]. Ənənəvi perimetr əsaslı kibermüdafiədən fərqli olaraq, kiberimmunitet daxili uyğunlaşma, konteksti nəzərə alma və dəyişən təhdidlərə cavab olaraq inkişaf etmək qabiliyyətinə malikdir [7]. Milli səviyyədə kiberimmunitet ancaq texniki sistemləri deyil, həmçinin institusional uyğunlaşmanı, hüquqi elastikliyi, strateji uzaqgörənliyi və ictimai hazırlığı əhatə edir [17].

Qeyd etmək lazımdlr ki, yuxarıda baxılan bu üç konsepsiya bir-birini istisna etmir və konseptual dayanıqlılıq təşkil edir. Belə ki, kibermüdafiə əsas mühafizə mexanizmləri, kiberdayanıqlılıq dayalılığı və bərpanı, kiberimmunitet isə uzunmüddətli sistem dayanıqlılığını artıran adaptiv, özü öyrənmə imkanlarını təqdim edir [8]. Cədvəl 1-də kibermüdafiə, kiberdayanıqlılıq və kiberimmunitet konsepsiyalarının müqayisəsi verilmişdir.

CƏDVƏL 1. KİBERMÜDAFİƏ, KİBERDAYANIQLILIQ VƏ KİBERİMMUNİTET KONSEPSİYALARININ MÜQAYİSƏSİ

Parametr	Kibermüdafiə	Kiberdayanıqlılıq	Kiberimmunitet
Strateji məqsəd	Hücumların qarşısının alınması və sistemlərin mühafizəsi	Hücum şəraitində sistem funksionallığının saxlanılması	Hücumların erkən aşkarlanması, öyrənilməsi və adaptiv müdafiə mexanizmlərinin formalaşdırılması
Yanaşmanın xarakteri	Reaktiv və perimetr yönümlü yanaşma	Adaptiv və davamlılıq yönümlü yanaşma	Proaktiv, adaptiv və özünü-öyrənən yanaşma
Əsas fəaliyyət sahəsi	Müdafiə mexanizmləri və insidentlərə cavab	Davamlı fəaliyyətin təmin edilməsi və operativ bərpa	Erkən aşkarlama, adaptasiya və immun yaddaşın formalaşdırılması
Zaman perspektivi	Qısamüddətli müdafiə tədbirləri	Orta və uzunmüddətli dayanıqlılıq strategiyaları	Uzunmüddətli, sistemli və evolyusion uyğunlaşma
Texnoloji baza	Firewall, IDS/IPS, antivirus və SIEM sistemləri	Ehtiyat infrastruktur, bərpa planları və dayanıqlılıq mexanizmləri	Süni intellekt, maşın təlimi və bio-əsaslı alqoritmlər
Hücuma reaksiyanın modeli	Hücumdan sonra cavab tədbirləri	Hücuma tab gətirmə və funksionallığın bərpası	Hücumun erkən aşkarlanması və adaptiv cavab
Öyrənmə və adaptasiya qabiliyyəti	Məhdud, əsasən qayda əsaslı	Qismən adaptiv	Davamlı öyrənən və özünü optimallaşdıran
Sistem davranış modeli	Statik və qayda əsaslı	Elastik və bərpa yönümlü	Dinamik, kontekst-şüurlu və adaptiv
İdarəetmə inteqrasiya səviyyəsi	Əsasən texniki səviyyə	Texniki və təşkilati səviyyələrin inteqrasiyası	Strateji, texniki və ictimai səviyyələrin kompleks inteqrasiyası
Bioloji analoq modeli	Mexaniki müdafiə sistemi	Stressə davamlı orqanizm modeli	Tam funksional immun sistem modeli

C. Beynəlxalq strategiyalar və çərçivələr

Milli kibertəhlükəsizlik siyasətlərinin formalaşdırması üçün müxtəlif beynəlxalq strategiya və çərçivə işlənilmişdir. Bu çərçivələr kiber risklərin idarə olunması və təhlükəsiz rəqəmsal ekosistemlərin qurulması üçün təlimatlar, ən yaxşı təcrübələr və standartlaşdırılmış yanaşmalar təqdim edir [12].

ABŞ Milli Standartlar və Texnologiya İnstitutu (NIST) tərəfindən NIST Kibertəhlükəsizlik Çərçivəsi hazırlanmışdır və strukturlaşdırılmış risk qiymətləndirməsi, hadisələrə cavab və davamlı monitorinq tösiyyələri təqdim edir. Bu çərçivə kibertəhlükəsizlik fəaliyyətlərini idarə et, müəyyən et, qoru, aşkarla, cavab ver və bərpa et kimi altı əsas funksiyaya bölür [18]. Bu risk əsaslı və çevik struktur dünya miqyasında hökumətlər və təşkilatlar tərəfindən kibertəhlükəsizlik idarəetməsi üçün təməl model kimi geniş şəkildə qəbul edilmişdir [9].

Avropa Birliyinin (AB) Kibertəhlükəsizlik Strategiyası kibertəhdidlərə qarşı dayanıqlılığı artırmaq, vətəndaşların və müəssisələrin etibarlı rəqəmsal texnologiyalardan faydalanmasını təmin etmək məqsədi daşıyır [19]. Avropa Birliyinin Kibertəhlükəsizlik Strategiyası və NIS2 Direktivi [20] üzv dövlətlər üçün tənzimləyici və əməliyyat tələblərini müəyyən edir. Bu təşəbbüslər şəbəkə və informasiya sistemlərinin təhlükəsizliyinin gücləndirilməsinə, ölkələrarası əməkdaşlığın gücləndirilməsinə və kritik infrastrukturların və vacib xidmətlərin kibertəhlükəsizliyinin təmin edilməsinə yönəlmişdir.

D. Milli kibertəhlükəsizliyin əsas çətinlikləri

Ədəbiyyatda milli kibertəhlükəsizlik sahəsində bir sıra çətinliklər ardıcıl olaraq müəyyən edilir [21]. Bu çətinliklərdən ən başlıcası qlobal kiber təhdidlərlə milli səviyyədə məhdudlaşdırılmış cavablar arasındakı asimmetriyadır [9]. Belə ki, kiberhücumlar tez-tez transmilli aktorlar tərəfindən həyata keçiridiyi halda, müdafiə tədbirləri əsasən milli hüquqi və institusional çərçivələr daxilində həyata keçirilir [3].

Digər bir mühüm problem kritik infrastrukturların mürəkkəbliyi və qarşılıqlı asılılığı ilə bağlıdır [1]. Müasir rəqəmsal ekosistemlər bir-biri ilə sıx bağlı olduğundan, bir sektordakı zəiflik digər sektorlara təsur edə bilər və bu sistemli qarşılıqlı əlaqə kiber insidentlərin potensial təsirini dəfələrlə artırmaqla yanaşı, risklərin idarə edilməsini çətinləşdirə bilər. Bundan başqa, kibertəhlükəsizlik mütəxəssislərinin çatışmazlığı da geniş şəkildə kritik problem kimi qəbul edilir. Bir çox ölkələr insan resurslarında əhəmiyyətli boşluqlarla üzləşir ki, bu da onların qabaqcıl kibertəhlükəsizlik tədbirlərini tətbiq etmək imkanlarını ciddi şəkildə məhdudlaşdırır. Əlavə olaraq, kibertəhdidlərin sürətli inkişafı ənənəvi statik müdafiə mexanizmlərin çox vaxt qeyri-effektiv edir.

Nəhayət, idarəetmə və koordinasiya problemləri əsas problemlərdən biri olaraq qalmaqdadır [14]. Belə ki, effektiv milli kibertəhlükəsizlik dövlət qurumları, özəl sektor və akademik qurumlar və həmçinin beynəlxalq tərəfdaşlar da daxil olmaqla bir çox maraqlı tərəflər arasında sıx əməkdaşlıq tələb edir.

III. MƏSƏLƏNİN QOYULUŞU

Dövlət idarəçiliyinin, kritik infrastrukturun, iqtisadi sistemlərin və sosial xidmətlərin sürətli rəqəmsallaşması müasir dövlətlərin əməliyyat mühitini kökündən dəyişmişdir. Bu transformasiyalar səmərəliliyi, qarşılıqlı əlaqəni və əlçatanlığı artırsa da, milli informasiya sistemlərinin hücum səthini də genişləndirib [1]. Nəticədə, kiberhücumlar miqyas və mürəkkəblik baxımından inkişaf edərək təkcə informasiya aktivləri üçün deyil, həm də milli təhlükəsizlik, iqtisadi sabitlik və ictimai rifah üçün strateji risklər yaratmışdır [3]. Bu vəziyyət ənənəvi kibertəhlükəsizlik yanaşmalarının yenidən qiymətləndirilməsini zəruri edir və daha adaptiv, sistemli və davamlı immunitet əsaslı yanaşmalara ehtiyac olduğunu göstərir [6]. Cədvəl 2-də ənənəvi kibertəhlükəsizlik və kiberimmun modellərinin müqayisəsi verilmişdir.

CƏDVƏL 2. ƏNƏNƏVİ KİBERTƏHLÜKƏSİZLİK VƏ KİBERİMMUN MODELLƏRİİNİN MÜQAYİSƏSİ

Meyar	Ənənəvi model	Kiberimmun modeli
Təhlükəsizlik yanaşmasının konseptual əsası	Perimetr yönümlü müdafiə (şəbəkə sərhədlərinin qorunmasına əsaslanır)	Davamlı və çoxsəviyyəli monitorinq
Reaksiya strategiyası	Reaktiv cavab (insident baş verdikdən sonra müdaxilə)	Adaptiv və proaktiv cavab strategiyası
Aşkarlama qaydaları	Statik qaydalar və imza-əsaslı aşkarlama	Anomaliya aşkarlanması və kontekst-əsaslı qərar qəbuletmə
İdarəetmə və nəzarət səviyyəsi	İnsan müdaxiləsi tələb olunur	Avtomatlaşdırılmış və intellektual cavab mexanizmləri
Öyrənmə və adaptasiya qabiliyyəti	Öyrənmə mexanizmi zəif və ya yoxdur	Özü öyrənən və adaptasiya
Hücumlara uyğunlaşma	Yeni hücumlara gecikmiş və məhdud reaksiya	Yeni və naməlum hücumlara dinamik uyğunlaşma
Sistem davranış modeli	Qoruyucu və statik	Dinamik, adaptiv və özünü bərpa
Məlumat analizinin	Qayda və imza əsaslı analiz	Davranış və anomaliya əsaslı analiz
Avtomatlaşdırma səviyyəsi	Məhdud avtomatlaşdırma imkanları	Yüksək səviyyədə avtomatlaşdırma

A. Müasir dövlətlərin üzləşdiyi kibertəhdidlər

Müasir kibertəhdidlər mürəkkəbliyi, müxtəlifliyi və strateji məqsədi ilə xarakterizə olunur. Bu gün dövlətlər inkişaf etmiş davamlı təhdidlər (APT), ransomware hücumları, dezinformasiya əməliyyatları və kiber casusluq da daxil olmaqla geniş çeşidli zərərli fəaliyyətlərlə üzləşirlər [4]. Bu təhdidlər sistemlərə sızmaq, aşkarlanmamaq və uzunmüddətli məqsədlərə çatmaq üçün mürəkkəb üsullardan istifadə edən yüksək dərəcədə mütəşəkkil cinayətkar qruplar və ya dövlət tərəfindən maliyyələşdirilən aktorlar tərəfindən həyata keçirilir [3].

Enerji, səhiyyə, maliyyə, nəqliyyat və dövlət xidmətləri kimi kritik sektorlar strateji əhəmiyyəti və genişmiqyaslı pozuntu potensialı səbəbindən əsas hədəflərə çevrilib [10]. Əməliyyat texnologiyaları (OT), Əşyaların İnterneti (IoT) cihazlarının və bulud əsaslı infrastrukturların artan inteqrasiyası təhlükəsizlik mənzərəsini daha da mürəkkəbləşdirib, bir-biri ilə əlaqəli sistemlərdə yeni zəifliklər və asılılıqlar yaradır [1].

B. Milli kibermüdafiədə struktur və təşkilati zəifliklər

Bu gün kiber-risklər barədə məlumatların artmasına baxmayaraq, bir çox milli kibertəhlükəsizlik sistemləri hələ də struktur və təşkilati məhdudiyyətlərə malikdir [11]. Bu zəifliklər çox vaxt zəif inteqrasiyaya malik idarəetmə strukturlarından, dövlət və özəl tərəflər arasında zəif koordinasiyadan və resursların qeyri-bərabər bölüşdürülməsindən qaynaqlanır [12].

Bir çox hallarda kibertəhlükəsizlik məsuliyyətləri bir-neçə qurum arasında bölüşdürülür ki, bu da mandatların üst-üstə düşməsinə, hesabatlılıqdakı boşluqlara və hadisələrə gecikmiş cavablara səbəb olur. Kritik infrastruktur operatorları, özəl şirkətlər və dövlət qurumları fərqli təhlükəsizlik standartlarına əməl edə bilər ki, bu da mühafizə səviyyələrində və hadisələrə cavab vermə imkanlarında uyğunsuzluqlar yaradır [12].

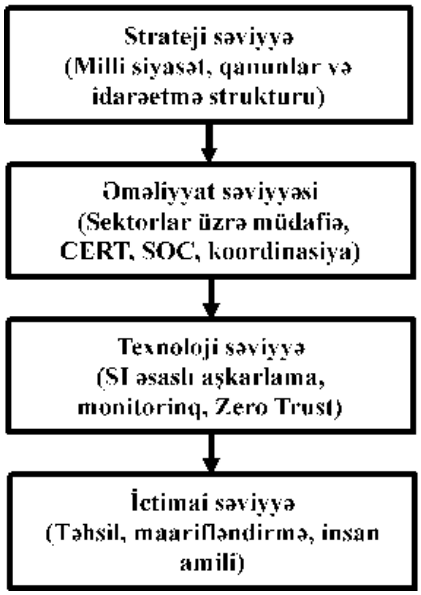
C. İnteqrasiya olunmuş və adaptiv kiberimmunitet modelinə ehtiyac

Ənənəvi kibertəhlükəsizlik yanaşmalarının məhdudiyyətləri nəzərə alınmaqla, dayanıqlılığa, uyğunlaşmaya və sistemli mühafizə təmin edən bir yanaşmaya artan ehtiyac var [6]. Kiberimmunitet anlayışı bu baxımdan perspektivli bir çərçivə təklif edir [7]. Bioloji immun sisteminə əsaslanan kiberimmunitet rəqəmsal ekosistemin anomaliyalarını aşkar etmək, yeni təhdidlərə uyğunlaşmaq və kiberhücumların nəticələrinin minimuma endirilməsi qabiliyyətinə malikdir [5].

İnteqrasiya olunmuş və adaptiv kiberimmunitet modeli vahid arxitektura daxilində kiberhücumların qarşısının aşkarlanması, alınması, cavablandırılması və kiberhücumdan sonra bərpa da daxil olmaqla bir-neçə müdafiə səviyyəsini birləşdirir [8]. Belə bir model davamlı öyrənmə və özünü optimallaşdırmanı təmin etmək üçün süni intellekt, maşın təlimi və bio-əsaslı alqoritmlər daxil olmaqla qabaqcıl analitik üsulları özündə birləşdirir [5].

IV. DÖVLƏTİN KİBERİMMUNİTET MODELİ

Müasir kibertəhdidlərin xüsusiyyətlərini nəzərə alaraq, dövlət kiberimmuniteti üçün inteqrasiya olunmuş model tələb olunur. Bu model strateji idarəetməni, texnoloji müdafiəni, insan potensialının inkişafını və beynəlxalq əməkdaşlığı vahid bir sistemə birləşdirməlidir [6]. Bunun üçün, model çoxsəviyyəli və adaptiv bir arxitekturaya malik olmalıdır. Təklif edilən model dövlət səviyyəsində kiberimmunitetin çoxsəviyyəli, inteqrasiya olunmuş və adaptiv arxitekturaya əsaslanır (Şəkil 1).



Şəkil 1. Modelin konseptual arxitekturası.

Strateji səviyyədə idarəetmə strukturları milli siyasətləri, hüquqi çərçivələri və koordinasiya mexanizmlərini müəyyən edir [9]. Əməliyyat səviyyəsində kritik infrastruktur sektorları üzrə təhlükəsizlik nəzarəti və dayanıqlılıq strategiyalarını tətbiq edilir [10]. Texnoloji səviyyədə monitorinq sistemləri, süni intellektlə idarə olunan aşkarlama mexanizmləri və sıfır etibar arxitekturaları kibertəhdidlərə qarşı davamlı mühafizəni təmin edir [22]. Nəhayət, ictimai səviyyədə təhsil və maarifləndirmə təşəbbüsləri vətəndaşlar və qurumların kibertəhlükəsizlik mədəniyyətin inkişafı dayanır [17].

Bu komponentlər arasında qarşılıqlı əlaqə dövlətin kiberimmunitetinin təmin edilməsi üçün çox vacibdir. Strateji siyasətlər texnoloji və təşkilati tədbirlərə rəhbərlik edir, monitorinq sistemlərindən alınmış məlumatlar isə strateji qərar qəbuletməni təmin edir. İnsan təcrübəsi həm texnoloji tətbiqi, həm də idarəetmə proseslərini dəstəkləyir, dinamik və qarşılıqlı əlaqəli müdafiə ekosistemini yaradır [11].

Təklif olunan modelin əsas xüsusiyyəti adaptiv və özü öyrənən təhlükəsizlik mexanizmlərinin inteqrasiyasından ibarətdir [5]. Bioloji immun sistemlərinə əsasıanan bu arxitektura davamlı monitorinq, anomaliya aşkarlanması, əks əlaqə və avtomatlaşdırılmış cavab imkanlarını özündə birləşdirir [7]. Bu mexanizmlər keçmiş hadisələr haqqında məlumata əsasən sistemin müdafiəsinin tənzimlənməsinə və yeni təhdidlərə daha effektiv cavab verilməsinə imkan verir.

Təklif edilən kiberimmunitet modeli, statik perimetr mühafizəsinə və reaktiv tədbirlərə əsaslanan ənənəvi kibertəhlükəsizlik yanaşmalarından fərqli olaraq, uyğunlaşma, dayanıqlılıq və sistemli koordinasiyanı birləşdirir [8]. Bu, təcrid olunmuş şəkildə ayrı-ayrı təşkilatların kibertəhlükəsizliyinin təmin edilməsi konsepsiyasından, milli səviyyədə mürəkkəb kiber təhdidləri qabaqcadan görə və azalda bilən inteqrasiya olunmuş, özünü inkişaf etdirən ekosistemə keçidi təmin edir [8].

V. DÖVLƏT KİBERİMMUNİTETİNİN YÜKSƏLDİLMƏSİ YOLLARI

Dövlətin kiberimmuniteti konsepsiyası ölkənin rəqəmsal ekosisteminin vacib funksiyalarını qoruyarkən kiber təhdidləri qabaqcadan görmək, onlara qarşı mübarizə aparmaq, qarşısını almaq və onlardan qaçmaq qabiliyyətini əks etdirir [6]. Kiberimmunitetin yüksəldilməsi idarəetməni, texnologiyanı, insan potensialını və beynəlxalq əməkdaşlığı birləşdirən konsepsiyaya əsaslanır [11].

A. Strateji və idarəetmə yanaşmaları

Strateji səviyyədə dövlət kiberimmunitetinin təməli hərtərəfli milli kibertəhlükəsizlik strategiyalarının işlənilməsi və həyata keçirilməsindən ibarətdir [9]. Bu cür strategiyalar milli prioritetləri və kritik riskləri müəyyən edir, qurumlar arasında məsuliyyətləri bölüşdürür və rəqəmsal infrastruktur və xidmətlərin mühafizəsi üçün uzunmüddətli məqsədlər müəyyən edir [12]. Milli strategiya bütün dövlət və özəl təşkilatların fəaliyyəti üçün rəhbər çərçivəni təmin edir.

Ümumiyyətlə, institusional koordinasiya effektiv kiber idarəetmənin əsas elementi sayılır [12]. Müasir kiber təhdidlər ənənəvi təşkilati və sektor sərhədlərini aşır və nazirliklər, tənzimləyici orqanlar, kəşfiyyat agentlikləri və kritik infrastruktur operatorları arasında əməkdaşlığa imkan verən inteqrasiya olunmuş idarəetmə modelləri tələb edir [11]. Milli kibertəhlükəsizlik mərkəzləri və ya kiber komanda strukturları kimi mərkəzləşdirilmiş koordinasiya orqanlarının yaradılması

daha səmərəli qərar qəbuletməyə və hadisələrə daha sürətli reaksiya verməyə kömək edir [14].

Bununla yanaşı, hüquqi və tənzimləyici çərçivələr kiberimmunitetin normativ əsasını təşkil edir [2]. Onlar dövlət və özəl qurumlar üçün təhlükəsizlik öhdəliklərini müəyyən edir, şəxsi və kritik məlumatların qorunmasını tənzimləyir və hadisələr barədə məlumat vermək və onlara cavab vermək üçün prosedurlar müəyyən edir [23]. Effektiv qanunvericilik sürətlə inkişaf edən təhlükə mühitində adaptiv, texnologiya baxımından neytral və beynəlxalq standartlara uyğun olmalıdır.

Dövlət və özəl təşkilatların tərəfdaşlıqları çox vacibdir, çünki kritik infrastrukturun və rəqəmsal xidmətlərin əhəmiyyətli bir hissəsi özəl təşkilatlara məxsusdur və ya onlar tərəfindən idarə olunur [10]. Məlumat paylaşma platformaları, birgə risk qiymətləndirmələri və əlaqələndirilmiş cavab tədbirləri daxil olmaqla əməkdaşlıq mexanizmləri qarşılıqlı etimadı artırır və milli kiber ekosisteminin ümumi dayanıqlılığını artırır [13].

B. Kritik infrastrukturların mühafizəsi

Kritik infrastrukturların mühafizəsi dövlət kiberimmunitetinin mərkəzi komponentidir, çünki vacib sektorlardakı fasilələr ciddi iqtisadi, sosial və milli təhlükəsizlik nəticələrinə səbəb ola bilər [10]. Bu prosesin ilk addımı enerji, nəqliyyat, səhiyyə, maliyyə, telekommunikasiya və dövlət xidmətləri kimi kritik infrastrukturların sistematik şəkildə müəyyən edilməsini və təsnif edilməsini əhatə edir.

Kritik aktivlər müəyyən edildikdən sonra dövlətlər hərtərəfli risk idarəetmə və dayanıqlılıq mexanizmlərini tətbiq etməlidirlər [15]. Buraya davamlı zəiflik qiymətləndirmələri, təhdid modelləşdirməsi və hər bir sektorun spesifik əməliyyat xüsusiyyətlərinə uyğunlaşdırılmış təhlükəsizlik standartlarının qəbul edilməsi daxildir. Kiberdayanıqlılığa yönəlmiş yanaşmalar yalnız kiberhücumlarının qarşısının alınmasını deyil, həm də kiberhücumlar zamanı və sonrası vacib funksiyaları qorumaq və ya tez bir zamanda bərpa etmək qabiliyyətini əhatə edir [16].

İnsidentlərə cavab və kiberdayanıqlılığın planlaşdırması eyni dərəcədə vacibdir [4]. Milli və müxtəlif sektorlara xas cavab planları aydın rolları, kommunikasiya kanallarını və bərpa prosedurlarını müəyyən etməlidir. Mütəmadi simulyasiyalar və stress testləri təşkilatlara kiberhücumlara hazırlıqlarını qiymətləndirməyə və maraqlı tərəflər arasında koordinasiyanı yaxşılaşdırmağa kömək edər [13].

C. Texnoloji tədbirlər

Texnoloji innovasiya dövlət kiberimmunitetinin əsas sütununu təşkil edir [22]. Müasir rəqəmsal infrastrukturlar hətta layihələndirmə mərhələlərində sistem arxitekturalarına inteqrasiya olunmuş kibertəhlükəsizlik mexanizmlərinin nəzərə alınmasını tələb edir. Bu, həmçinin sistemin yaradılmasının bütün dövrü ərzində kibertəhlükəsizlik nəzarətinin, risk qiymətləndirmələrinin və təhdid modelləşdirməsinin daxil edilməsini nəzərdə [1].

Sıfır etibar arxitekturası ənənəvi perimetr əsaslı kibertəhlükəsizlik modellərindən fərqlənir [24]. Şəbəkə sərhədləri daxilində sıfır etibar yanaşmaları istifadəçilərin, avadanlıqların və proseslərin davamlı yoxlanılmasını tələb edir. Bu model hücum edənlər tərəfindən qeyri-qanuni fəaliyyət riskini azaldır və milli rəqəmsal infrastrukturlarının ümumi kibertəhlükəsizlik səviyyəsini artırır.

Süni intellekt (Sİ) və adaptiv müdafiə mexanizmlərinin inteqrasiyası kibertəhdidlərin proaktiv aşkarlanması və cavablandırılması üçün yeni imkanlar təqdim edir [5]. Sİ əsaslı sistemlər böyük həcmdə şəbəkə və sistem məlumatlarını təhlil edə, anomaliyaları aşkarlaya və inkişaf edən kibertəhdidlərə cavab olaraq davranışlarını uyğunlaşdıra bilər. Bu cür mexanizmlər özü öyrənən və özünü sağaldan kibertəhlükəsizlik mühitlərinin yaradılmasına töhfə verir [6].

Milli kibermonitorinq və erkən xəbərdarlıq sistemləri kibertəhlükəsizlik barədə məlumatlılığı artırır [16]. Bu sistemlər birdən çox sektordan və mənbələrdən məlumatları birləşdirərək, ortaya çıxan kibertəhdidlərin və əlaqələndirilmiş kiberhücumların aşkarlanmasına imkan verir. Erkən xəbərdarlıq imkanları qərar qəbul edənlərə milli səviyyədə profilaktik tədbirlər həyata keçirməyə və cavabları əlaqələndirməyə imkan verir.

D. İnsan faktoru və kibertəhlükəsizlik mədəniyyəti

Texnoloji tədbirlər vacib olsa da, insan amili kiberimmunitetin ən əhəmiyyətli elementlərindən biri olaraq qalır [13]. Çünki, bir çox kiber insidentlər insan səhvlərindən, məlumatsızlıqdan və ya təşkilati təcrübəsizlikdən qaynaqlanır [4]. Buna görə də, həm institusional, həm də ictimai səviyyələrdə güclü kibertəhlükəsizlik mədəniyyətinin olması çox vacibdir.

Kibertəhlükəsizlik sahəsində təhsil və işçi qüvvəsinin inkişafı ixtisaslı mütəxəssislərin çatışmazlığının aradan qaldırılmasında mühüm rol oynayır [13]. Dövlətlər bacarıqlı kibertəhlükəsizlik işçi qüvvəsi yetişdirmək üçün ixtisaslaşmış akademik proqramlara, peşə təliminə və davamlı peşəkar inkişaf təşəbbüslərinə investisiya qoymalıdırlar. Universitetlər, sənaye və dövlət qurumları arasında əməkdaşlıq təhsil səviyyəsinin praktik ehtiyaclarla uyğunlaşdırmağa kömək edə bilər.

Vətəndaşlar və dövlət qulluqçuları üçün maarifləndirmə proqramlarının olması da çox vacibdir [17]. İctimai kampaniyalar, təlim sessiyaları və rəqəmsal savadlılıq təşəbbüsləri sosial mühəndislik hücumları, fişinq və digər insan yönümlü kibertəhdidlər riskini azalda bilər.

Təşkilat səviyyəsində kibermədəniyyətin yüksəldilməsi işçilərin kibertəhlükəsizlik siyasətini necə qəbul etdiyinə və onlara necə reaksiya verdiyinə təsir göstərir [11]. Şəffaflığı, hesabatlılığı və davamlı öyrənməni təşviq edən təşkilatlar kibertəhdidlər qarşısında daha davamlı davranış nümayiş etdirmə ehtimalı daha yüksəkdir [13].

E. Beynəlxalq əməkdaşlıq və kollektiv kiber müdafiə

Kibertəhdidlərin transmilli təbiətə malik olduğu üçün, heç bir dövlət təcrid olunmuş şəkildə kiberimmuniteti təmin edə bilməz [3]. Buna görə də beynəlxalq əməkdaşlıq milli kiberdayanıqlılığın vacib bir elementidir. Dövlətlər arasında məlumat mübadiləsi təhdid kəşfiyyatı, zəiflik məlumatları və

ən yaxşı təcrübələrin sürətli mübadiləsinə imkan verir və bununla da kollektiv müdafiə imkanlarını gücləndirir [13].

Beynəlxalq kibertəhlükəsizlik təşəbbüslərində, ittifaqlarında və standartlaşdırma səylərində iştirak dövlətlərə siyasətlərini beynəlxalq norma və çərçivələrə uyğunlaşdırmağa və ortaq təcrübədən faydalanmağa kömək edir [9]. Regional və qlobal çərçivələrdə iştirak, dövlətlərə kibertəhlükəsizlik potensialın yüksəldilməsinə və strateji koordinasiyaya töhfə verir.

Birgə cavab mexanizmləri və kiber diplomatiya dövlətlərin kiberimmunitetinin yüksəldilməsində mühüm rol oynayır [3]. Birgə təlimlər və insidentlərin idarə olunması çərçivələri daxil olmaqla, genişmiqyaslı kiberinsidentlərə əlaqələndirilmiş cavablar iştirakçı dövlətlər arasında etimadı və əməliyyat hazırlığını artırır. Kiber diplomatiya, öz növbəsində, beynəlxalq normaların, etimad qurucu tədbirlərin və kiber münaqişə riskini azaltmağa yönəlmiş razılaşmaların işlənilməsinə imkan verir [2].

NƏTİCƏ

Bu məqalədə dövlətin kiberimmuniteti konsepsiyası araşdırılmış və müasir rəqəmsal mühit kontekstində onun gücləndirilməsi üçün əsas istiqamətlər müəyyən etmişdir. Təhlil göstərdi ki, milli səviyyədə effektiv kibertəhlükəsizlik texnoloji müdafiəni, institusional koordinasiyanı, hüquqi çərçivələri və insan kapitalının inkişafını birləşdirən inteqrasiya olunmuş və adaptiv yanaşma tələb edir [6]. Dövlətlər kibertəhdidləri qabaqcadan görə bilən, inkişaf edən risklərə uyğunlaşan, adaptiv, proaktiv, özü öyrənən və öz-özünü bərpa imkanlarına malik sistemlər qurmalıdırlar [5].

Dövlətin kiberimmunitetinin yüksəldilməsinin əsas istiqamətlərinə kritik infrastrukturun davamlı inkişafı, vahid milli kibertəhlükəsizlik strategiyalarının tətbiqi, kiber mühit barədə məlumatlılığın artırılması və insidentlərə cavab və bərpa üçün effektiv mexanizmlərin yaradılması daxildir [9]. Bundan əlavə, kiberdayanıqlılığın uzunmüddətli təmin edilməsi üçün təhsilə, işçi qüvvəsinin inkişafına və tədqiqata investisiya qoyuluşu vacibdir [17].

Siyasət baxımından hökumətlər hərtərəfli hüquqi və tənzimləyici çərçivələrin yaradılmasına, təşkilatlararası əməkdaşlığın təşviqinə və beynəlxalq tərəfdaşlıqların genişləndirilməsinə üstünlük verməlidirlər [2]. Eyni zamanda, tədqiqat səyləri adaptiv təhlükəsizlik modellərinə, süni intellektlə idarə olunan kibertəhdidlərin aşkarlanmasına və kiber-fiziki sistemlərin mühafizəsinin milli strategiyalara inteqrasiyasına yönəlməlidir [22].

Gələcək tədqiqatlar kiberimmunitet modellərinin praktiki təsdiqlənməsini, milli kibertəhlükəsizlik strategiyalarının müqayisəli analizini və dövlət səviyyəsində kiberdayanıqlılığın qiymətləndirilməsi üçün kəmiyyət göstəricilərinin işlənilməsini əhatə etməlidir [9]. Bundan başqa, süni intellekt, kvant hesablamaları və mərkəzləşdirilməmiş arxitekturalar kimi inkişaf etməkdə olan texnologiyaların növbəti nəsil milli kibertəhlükəsizlik sistemlərinin formalaşmasındakı rolunu araşdırılmalıdır [1]. Nəticədə, dövlətin kiberimmunitet anlayışı milli kibertəhlükəsizliyin yüksəldilməsi üçün praktik və ölçülə bilən bir çərçivəyə çevrilə bilər.

ƏDƏBİYYAT

[1] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: state of the art, challenges and future directions," Cyber Security and Applications, vol. 2, p. 100031, 2024. https://doi.org/10.1016/j.csa.2023.100031.

[2] W. Heintschel von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace," in Proc. 4th Int. Conf. Cyber Conflict, Tallinn, Estonia, 2012, pp. 7--19.

[3] A. Adeyeri and H. Abroshan, "Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era," Information, vol. 15, no. 11, p. 682, Nov. 2024. https://doi.org/10.3390/info15110682.

[4] I. Nallick, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," World Scientific News, vol. 190, no. 1, pp. 1--69, 2024.

[5] O. I. Falowo, L. E. Botsyoe, K. Koshoedo, and M. Ozer, "Enhancing Cybersecurity With Artificial Immune Systems and General Intelligence: A New Frontier in Threat Detection and Response," IEEE Access, vol. 12, pp. 122312--122323, 2024. https://doi.org/10.1109/ACCESS.2024.3454543.

[6] K. Tallam, "The Cyber Immune System: Harnessing Adversarial Forces for Security Resilience," EECS, University of California at Berkeley, Feb. 2025.

[7] S. A. Petrenko, K. A. Makoveichuk, and A. V. Olifirov, "Concept of Cyber Immunity of Industry 4.0," in Proc. 2019 Conf., 2019. https://doi.org/10.1109/ElConRus.2018.8317245.

[8] Kaspersky, "A Cyber Immunity-based approach to information system security," KasperskyOS White Paper.

[9] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," Comput. Secur., vol. 120, art. no. 102820, Sep. 2022. https://doi.org/10.1016/j.cose.2022.102820.

[10] O. O. Val, T. M. Kolade, M. O. Gbadebo, O. Selesi-Aina, O. O. Olateju, and O. O. Olaniyi, "Strengthening cybersecurity measures for the defense of critical infrastructure in the United States," Asian Journal of Research in Computer Science, vol. 17, no. 11, pp. 25-45, 2024. https://doi.org/10.9734/ajrcos/2024/v17i11517.

[11] M. Dunn Cavelty and F. J. Egloff, "The Politics of Cybersecurity: Balancing Different Roles of the State," St Antony's International Review, vol. 15, no. 1, pp. 37--57, 2019.

[12] M. Baezner and S. Cordey, "National Cybersecurity Strategies in Comparison - Challenges for Switzerland," Center for Security Studies (CSS), ETH Zürich, Zurich, Switzerland, Mar. 2019.

[13] J. Bellasio, R. Flint, N. Ryan, S. Sondergaard, C. G. Monsalve, A. S. Meranto, and A. Knack, "Developing Cybersecurity Capacity: A proof-of-concept implementation guide," RAND Corporation, Santa Monica, Calif., USA, Rep. RR-2072, 2018. www.rand.org/t/RR2072

[14] A. Sutomo, A. Octavian, P. Widodo, and Y. Reksoprodjo, "Integration strategy of cyber defense with national cyber security to maintain state sovereignty," Jurnal Pertahanan, vol. 7, no. 2, pp. 1-12, 2021.

[15] K. Nandini, A. Yaramsetty, and M. Tulasirama, "Enhancing cybersecurity resilience: a study of threat detection and mitigation techniques in modern networks," Library Progress International, vol. 44, no. 3, pp. 12371-12380, 2024.

[16] H. Kavak, J. J. Padilla, D. Vernon-Bido, S. Y. Diallo, R. Gore, and S. Shetty, "Simulation for cybersecurity: state of the art and future directions," Journal of Cybersecurity, vol. 7, no. 1, pp. 1-13, 2021. https://doi.org/10.1093/cybsec/tyab005.

[17] E. B. Sobirjonovich, "Cybersecurity and Social Consciousness: Concepts of Immunity Formation," Scientia Journal of Economics, Humanities and Social Sciences, vol. 2025, no. 4, pp. 1--5, Apr. 2025.

[18] National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper (CSWP) NIST CSWP 29, Gaithersburg, MD, 2024. doi: 10.6028/NIST.CSWP.29. [Online]. https://doi.org/10.6028/NIST.CSWP.29

[19] EU Cybersecurity Strategy. https://digital-strategy.ec.europa.eu/en/-policies/cybersecurity-strategy

[20] NIS2 Directive: securing network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[21] W. S. Admass, Y. Y. Munay, and A. Diro, "A state-of-the-art review on cybersecurity: Challenges and opportunities," Journal of Cybersecurity, 2023. https://doi.org/10.1016/j.jksuci.2021.01.018.

[22] M. Danish, "Enhancing cyber security through predictive analytics: real-time threat detection and response," International Journal of Advanced Computer Science and Applications, vol. 16, no. 8, pp. 43-54, 2025. [Online]. Available: arXiv:2407.10864v2.

[23] W. Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," International Law Studies, vol. 89, pp. 123--156, 2013.

[24] H. L. Gururaj, M. Spoorthi, V. Ravi, S. J, and K. S. Roy, "Securing the Future: Introduction to Zero Trust in Cybersecurity," Manipal Academy of Higher Education, India..

A Study of Ways to Enhance State Cyberimmunity

Ramiz Shikhaliyev

Institute of Information Technology, Baku, Azerbaijan

Abstract— Today, information and communication technologies (ICT) are widely used in the governance, economic, social, and security systems of states. The rapid development of ICT has led to the emergence of complex, multi-vector, and artificial intelligence–based cyberattacks. Traditional reactive defense models are not very effective against these cyber threats. Therefore, cyberimmunity has become a strategic approach that ensures the cybersecurity of state information systems through adaptive, proactive, and self-learning mechanisms. Based on the principles of biological immune systems, state cyberimmunity combines early detection, adaptive response, immune memory, and self-healing capabilities, enabling the protection of national cyber sovereignty. This article analyzes the characteristics of existing cyber threats, the limitations of traditional reactive cybersecurity approaches, and explores ways to enhance state cyberimmunity.

Keywords— cyberimmunity; cybersecurity; cyber sovereignty; cyber resilience; adaptive defense; bio-inspired cyber defense.