AZƏRBAYCAN RESPUBLİKASI

Əlyazması hüququnda

RƏQƏMSALLAŞMA DÖVRÜNDƏ KİBERTƏHLÜKƏSİZLİYİN SOSİAL VƏ SİYASİ ASPEKTLƏRİ

İxtisas: 5901.01 – "Beynəlxalq münasibətlər"

Elm sahəsi: Siyasi elmlər

İddiaçı: **Kəmilə Famil qızı Cabbarova**

Fəlsəfə doktoru elmi dərəcəsi
almaq üçün təqdim edilmiş dissertasiyanın

AVTOREFERATI

Bakı – 2026

Dissertasiya işi Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyasının Beynəlxalq münasibətlər kafedrasında yerinə yetirilmişdir.

Elmi rəhbər: siyasi elmlər doktoru, professor
Elman Xudam oğlu Nəsirov

Rəsmi opponentlər: siyasi elmlər doktoru, professor
Hicran Kamran qızı Hüseynova

siyasi elmlər üzrə fəlsəfə doktoru, dosent
Zümrüd Eldar qızı Məlikova

siyasi elmlər üzrə fəlsəfə doktoru, dosent
Pərvanə Telman qızı Mustafazadə

Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyasının Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyası nəzdində fəaliyyət göstərən FD 2.30 Dissertasiya şurası.

Dissertasiya şurasının sədri: _____ akademik **Urxan Kazım oğlu Ələkbərov**

Dissertasiya şurasının elmi katibi: _____ siyasi elmlər doktoru, professor **Sevda Ağamirzə qızı Əliyeva**

Elmi seminarın sədri: _____ siyasi elmlər doktoru, professor **Elçin İldırım oğlu Əhmədov**

İŞİN ÜMUMİ SƏCİYYƏSİ

Mövzunun aktuallığı və işlənmə dərəcəsi. XXI əsrdə rəqəmsal texnologiyaların sürətli inkişafı beynəlxalq münasibətlərin mahiyyətini və qlobal təhlükəsizlik arxitekturasını kökündən transformasiyaya uğratmışdır. Müasir dövrdə kiberməkan dövlətlərin, beynəlxalq təşkilatların və transmilli korporasiyaların strateji maraqlarının kəsişdiyi yeni bir geosiyasi rəqabət poliqonuna çevrilmişdir. Bu müstəvidə formalaşan yeni güc konfiqurasiyası informasiya resurslarını aktiv və həlledici strateji kapital statusuna yüksəldir.

İctimai həyatın bütün sahələrinin rəqəmsallaşdırılması kibermüharibə, kibercasusluq, kiberterrorizm və dezinformasiya kampaniyaları da daxil olmaqla, tamamilə yeni qarşıdurma formalarına səbəb olur. Bu hadisələr vacib infrastrukturun fəaliyyəti ilə yanaşı, həm də gücün legitimliyinə, ictimai etimada və beynəlxalq qurumların sabitliyinə təsir göstərir. Bu genişmiqyaslı təsirin kökündə isə müasir qarşıdurmaların xarakterinin köklü surətdə dəyişməsi dayanır. Müasir münaqişələr getdikcə hərbi, siyasi, iqtisadi və informasiya alətlərinin bir-biri ilə əlaqəli olduğu hibrid formada inkişaf edir. Bu kontekstdə kibertəhlükəsizlik milli gücün və diplomatiyanın ayrılmaz elementinə çevrilir və hərtərəfli təhlil tələb edir ki, bu da mövzunun aktuallığını şərtləndirir.

Rəqəmsal təhlükəsizlik tədqiqatlarının artmasına rəğmən, kibertəhdid və kibermüharibə fenomenlərinin konseptual əsasları fraqmentləşmişdir. Beynəlxalq münasibətlər nəzəriyyəsində realist paradiqma kiberməkanı dövlət suverenliyinin və hərbi gücün yeni arenası, liberal yanaşma hüquqi normalar və kollektiv əməkdaşlıq platforması, konstruktivist interpretasiyalar isə strateji diskurs və identifikasiya faktorlarının məhsulu kimi nəzərdən keçirir. Eləcə də, müasir elmi dövriyyədə siyasi determinizm, texnoloji konfiqurasiya və sosial dinamikaların kibertəhlükəsizlik ekosistemlərinə kompleks təsirini izah edən holistik konseptual çərçivəyə ciddi ehtiyac duyulur. Bu boşluğun doldurulması tədqiqatın aktuallığını şərtləndirir.

Süni intellekt siyasi və ictimai sahələrə dərindən nüfuz edir. O, idarəetməni yaxşılaşdırsa da, dezinformasiya, manipulyasiya və konfidensiallığın pozulması kimi etik, hüquqi təhdidlər yaradır. Siyasi müstəvidə isə böyük verilənlərin təhlili seçici davranışlarını

proqnozlaşdırmağa və hədəfli "mikrohədəfləmə" strategiyaları qurmağa imkan verir. Lakin bu inkişaf kibertəhlükəsizlik anlayışını yalnız texniki infrastrukturun qorunmasından çıxararaq, onu informasiya təhlükəsizliyi və psixoloji müharibə müstəvisinə daşımışdır. Xüsusilə "deepfake" texnologiyaları və generativ süni intellekt modelləri vasitəsilə yaradılan saxta məzmunlar seçki dürüstlüyünə və ictimai etimada birbaşa zərbə vurur. 2016-cı il ABŞ prezident seçkilərində baş vermiş "Cambridge Analytica" qalmaqalı və Hindistandakı 2024-cü il seçkiləri zamanı deepfakelərin yayılması süni intellektin siyasi manipulyasiya alətinə çevrilməsinin qlobal risklərini aydın şəkildə nümayiş etdirir və mövzunu aktual edir.

44 günlük Vətən müharibəsi dövründə informasiya üstünlüyünün əldə edilməsi üçün süni intellekt əsaslı Tavush Bot kimi alətlərin tətbiqi informasiya müharibəsinin yeni paradiqmasını ortaya qoymuşdur. Azərbaycanda qəbul edilmiş "2023–2026-cı illər üçün Rəqəmsal Transformasiya Strategiyası" süni intellektin dövlət idarəetməsində tətbiqini prioritet elan etməklə, bu texnologiyaların etik və şəffaf istifadəsini gündəmə gətirir. Beləliklə, Sİ əsaslı kibertəhdidlərin siyasi və sosial aspektlərinin tədqiqi milli təhlükəsizlik strategiyasının formalaşdırılması baxımından müstəsna əhəmiyyət daşıyır və mövzunu aktual edir.

Dissertasiya mövzusu Azərbaycanın siyasi-elmi fikrində ilk dəfə kompleks şəkildə tədqiqata cəlb olunur. Problemin beynəlxalq siyasi təfəkkürdə də sistemli şəkildə araşdırılmaması onun elmi aktuallığını artırır və dərinləşdirilmiş təhlilini zəruri edir. Bununla belə, tədqiqat obyektinin ayrı-ayrı aspektləri müxtəlif xarici müəlliflərin araşdırmalarında bu və ya digər dərəcədə əksini tapmışdır. Bu baxımdan, mövcud elmi ədəbiyyatı mövzu ilə bağlılıq dərəcəsinə görə bir neçə təsnifat qrupuna ayırmaq mümkündür. Birinci qrupda A.S.Arslan, R.O.Keohane, J.S.Nye[1] və digər

[1] Arslan, A.S. Neorealist Analysis of Security Dilemma in Cyberspace: A Quantitative Study // Political Theory, – 2024. Version 10: [Electron resource] / URL: https://www.researchgate.net/publication/ 380387742_ Neorealist_Analysis_ of_Security_Dilemma_in_Cyberspace_A_Quantitative_Study; Keohane, R.O. Power and Interdependence: World Politics in Transition / R.O.Keohane, J.S.Nye. – Boston: Little, Brown, – 1977. – 273 p.; Nye, J.S. Cyber Power / J.S.Nye. – Belfer Center, – 2010. – 28 p.

müəlliflər kiberməkanı klassik beynəlxalq münasibətlər nəzəriyyələri prizmasından; ikinci qrupda L.Alford, G.Bayraktar, B.Buchanan və digər müəlliflərin araşdırmaları kiberəməliyyatların hərbi, strateji tərəfləri və dövlətlərarası münaqişələri; üçüncü qrupda V.Boulanin, E.Blessing, M.Ashok, C.Cupać[2] və digərləri süni intellektin təhlükəsizlik sahəsindəki rolu, etik problemlər və hüquqi çərçivələri; dördüncü qrupda C.Hadnagy, J.Owen[3] və digərləri kiberməkanda manipulyasiya, dezinformasiya mövzularını; beşinci qrupda A.Barrinha, S.Arséne[4], A.Chander, R.Creemers, S.Couture, L.DeNardis, L.Floridi, E.Izycki və digərlərinin tədqiqatlarında dövlətlərin internet üzərində nəzarəti, məlumat millətçiliyi və qlobal idarəçilik modelləri tədqiq edilmişdir.

Tədqiqatın obyekti və predmeti. Tədqiqatın **obyekti** təhlükəsizlik fenomeninin ümumi sistemi, **predmeti** rəqəmsallaşma dövründə kibertəhlükəsizlikdir. Tədqiqatın məqsədi rəqəmsallaşma dövründə kibertəhlükəsizliyin sosial və siyasi aspektlərinin kompleks təhlilidir. Məqsədə nail olmaq üçün aşağıdakı konkret vəzifələrin yerinə yetirilməsi nəzərdə tutulur:

- Siyasi elmlər kontekstində "kibertəhlükəsizlik" fenomeninin konseptual çərçivəsini və onun milli təhlükəsizlik arxitekturasında tutduğu mövqeyi müəyyən etmək;

---

[2] Boulanin, V. Mapping the Development of Autonomy in Weapon Systems / V.Boulanin, M.Verbruggen // Stockholm International Peace Research Institute (SIPRI), – 2017.; Ashok, M. Ethical framework for Artificial Intelligence and Digital technologies / M.Ashok, R.Madan, A.Joha, U.Sivarajah // International Journal of Information Management, – 2022; Cupać, J. Regulate against the machine: how the EU mitigates AI harm to democracy / J.Cupać, M.Sienknecht // Democratization, – 2024, Vol.31, Issue: 5, – pp.1067–1090.

[3] Hadnagy, C. Social Engineering: The Science of Human Hacking / C.Hadnagy. – Wiley. Canada, – 2018. – 354 p; Owen, J. Psychological Mechanisms in Social Engineering Attacks // EasyChair. – 2024.

[4] Arséne, S. La Chine et le contrôle d'Internet: une cybersouveraineté à multiples facettes // Annuaire français de relations internationales, – 2022, – pp. 959–976; Creemers, R. Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management // Journal of Contemporary China, – 2016, – pp. 85–100; Floridi, L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU // Philosophy & Technology, – 2020, Vol.33, Issue 3 – pp.369–378; Izycki, E. National Cyber Security Strategies in Latin America: Opportunities for Convergence of Interests and Consensus Building, – 2018.

- Kibertəhlükəsizliyin siyasi analizi üçün tətbiq edilən aparıcı metodoloji prinsipləri və tədqiqat çərçivələrini sistemləşdirmək;

- Rəqəmsal dövrün kibertəhlükəsizlik çağırışlarını klassik və modern Beynəlxalq Münasibətlər nəzəriyyələri prizmasından kompleks şəkildə təhlil etmək;

- Qeyri-kinetik müharibələrin mahiyyətini, onların hərəkətverici qüvvələrini və regional təhlükəsizlik dinamikalarına təsirini araşdırmaq;

- Milli kibertəhlükəsizlik siyasətinin formalaşması prosesini, "rəqəmsal suverenlik" konsepsiyasını və beynəlxalq əməkdaşlıq mexanizmlərini qarşılıqlı əlaqədə təhlil etmək;

- Sosial mühəndislik fenomenini nəzəri və praktiki aspektdə araşdıraraq, kibertəhlükəsizliyin psixoloji-davranış parametrlərini müəyyən etmək;

- Kiberqavrayış nəzəriyyəsindən çıxış edərək, milli rəqəmsal immunitetin formalaşdırılmasında koqnitiv davamlılığın strateji əhəmiyyətini əsaslandırmaq;

- Rəqəmsal nəzarət və kibertəhlükəsizlik sistemlərində Sİ texnologiyalarının tətbiqi zamanı dövlətin tənzimləyici rolunu və hüquqi-siyasi məsuliyyətini müəyyənləşdirmək;

- Süni İntellektin və avtonom sistemlərin yaratdığı siyasi-etik dilemmaları, eləcə də bu texnologiyaların beynəlxalq təhlükəsizlik mühitində yaratdığı fundamental transformasiyaları analiz etmək.

Tədqiqat metodları. Dissertasiya işinin nəzəri bazasını beynəlxalq münasibətlərin müasir modellərini və terminoloji aparatını formalaşdıran xarici müəlliflərin konseptual yanaşmaları təşkil edir. Tədqiqatın nəzəri çərçivəsi formalaşdırılarkən J.Roozenbeek və S.Van der Linden, R.Jervis, J.S.Nye, L.Kello, K.N.Waltz, H.Morgenthau, B.Buzan, K.Jørgensen, R.Keohane, H.Özdemir, İ.Danilin, S.Shekhawat, N.Choucri, F.Kramer, A.Krishnan, J.Snyder, P.Singer, M.Libicki və V.Güntay kimi müəlliflərin əsərlərində irəli sürülən metodoloji prinsiplərə istinad edilmişdir.

Tədqiqatın metodoloji bazasını materialist dialektika, sistemli yanaşma və 1.2. paraqrafında şərh olunan elmi çərçivələr təşkil edir. İşdə ümumi metodlarla yanaşı, təhdidlərin sabitliyə təsirini ölçən

siyasi risk analizi, dinamik meyilləri proqnozlaşdıran ssenari planlaşdırılması və kiberinsidentləri dərindən araşdıran case-study metodlarından istifadə olunmuşdur (cədvəl 1).

Cədvəl 1

Beynəlxalq münasibətlərin əsas paradiqmaları və kibertəhlükəsizlikdə nəzəri yanaşmaların təhlil sxemi

Beynəlxalq əlaqələrə dair üç paradiqma	Siyasi düşüncə strukturları	Təhlilin ilkin səviyyəsi	İzahedici elementlər
Realizm (gerçəklik)	İnsan qrupları	Dövlətlərarası səviyyə	Hərbi güc balansı
Rasionalizm	Rasional aktorlar	Fərdi səviyyə	Danışıqlar, maraqlar
İnqilabçılıq	Kapitalist sistemə tənqidi yanaşma	Qlobal sistem səviyyəsi	Struktur gücü və iqtisadi asılılıqlar

Mənbə: *Cədvəl dissertasiya işinin I fəslində aparılan müqayisəli təhlillər əsasında müəllif tərəfindən tərtib edilmişdir.*

Tədqiqatın mənbə bazası. Mövzunun siyasi, hüquqi və praktiki aspektlərinin kompleks təhlili məqsədilə geniş sənəd bazasından istifadə edilmişdir. Tədqiqatın normativ-hüquqi əsaslarını Budapeşt Konvensiyası, NATO-nun Kibermüdafiə Öhdəliyi, Aİ-nin NIS2 Direktivi və "Rəqəmsal Onillik" Strategiyası, həmçinin Azərbaycan Respublikasının 2023–2027-ci illər üzrə Kibertəhlükəsizlik və 2025–2028-ci illər üzrə Süni İntellekt strategiyaları təşkil edir. İşin empirik-analitik bazası formalaşdırılarkən Qlobal Kibertəhlükəsizlik İndeksi (2025), Milli Kiber Güc İndeksi (2022), Microsoft-un Rəqəmsal Müdafiə Hesabatı (2025), Tallinn Təlimatı 2.0 və BMT-nin kiberməkanda məsuliyyətli dövlət davranışına dair hesabatlarına istinad edilmişdir.

Tədqiqatın elmi əhəmiyyətini müəyyənləşdirən və müdafiəyə təqdim olunan **müddəalar** aşağıdakı kimi qruplaşdırılmışdır:

Suverenliyin və beynəlxalq münasibətlərin yeni paradiqması

1. Dövlət suverenliyinin klassik modeli coğrafi məkandan rəqəmsal sahəyə transformasiya olunaraq "Rəqəmsal Vestfal"

paradiqması müstəvisinə keçmişdir. Müasir dövlətin hüdudları coğrafi koordinatlarla funksional olaraq "alqoritmik nəzarət" və "data-yurisdiksiyası" ilə yenidən formalaşır.

2. Dövlətin funksional varlığı yalnız coğrafi ərazi bütövlüyü ilə deyil, həm də xarici yurisdiksiyalarda qorunan kritik verilənlər (bulud vahidi və data-səfirlikləri) vasitəsilə təmin olunur. Bu, beynəlxalq hüquqda suverenliyin bölünməzliyi prinsipinə eksterritorial mahiyyət qazandırır.

3. Milli gücün klassik DIME modeli "koqnitiv sahədə ortaq həqiqəti müdafiə etmək" bacarığı ilə tamamlanır. Azərbaycanın rəqəmsal ekosistemdə həm "sahibkar", həm də "tənzimləyici" funksiyalarını sintez edən aktiv hibrid dövlət modeli milli təhlükəsizliyin yeni suverenlik formatını təşkil edir.

Geosiyasi dinamikalar və regional təhlükəsizlik

1. Regional kibertəhdidlərin təsnifatı Rusiya modelinin "total rəqəmsal müharibə" və İran modelinin "daimi asimmetrik sabotaj" profilləri üzərində qurulur. Bu təsnifat hibrid təhdidlərin sosial sabitliyə təsir dərəcələrini proqnozlaşdıran əsas analitik çərçivədir.

2. Azərbaycanın geosiyasi mövqeyi "kibertranzit suverenliyi" faktoru ilə müəyyən edilir. "Rəqəmsal İpək Yolu" layihəsi ölkəyə regionda kibertəhlükəsizlik standartlarını diktə edən "normativ güc" statusu və strateji suverenlik üstünlüyü qazandırır.

3. Qlobal internetin parçalanması şəraitində milli rəqəmsal ekosistemin dayanıqlılığı, mütləq suverenlik prinsipləri ilə beynəlxalq rəqəmsal dövriyyənin sintezinə əsaslanan "hibrid lokallaşdırma" idarəetmə modeli vasitəsilə təmin olunur.

Koqnitiv dözümlülük və sosial-siyasi sabitlik

1. Kibermaarifləndirmə milli təhlükəsizliyin birinci müdafiə xətti olan "idraki immunitet" səviyyəsinə yüksəlmişdir. Bu doktrina dövlət rəhbərliyi və cəmiyyət üçün manipulyasiyanı bloklayan əsas "strateji filtr" rolunu oynayır.

2. Sosial mühəndislik əməliyyatları dövlətin qərarvermə mexanizmini məhz "Səmtlənmə" mərhələsində manipulyasiya edir. Bu, kiberatributasiya problemini texniki maneədən dövləti yanlış geosiyasi qərarlara sövq edən idraki maneəyə çevirir.

3. Kibertəhlükəsizlik dövlətin siyasi legitimliyinin qorunması

və vətəndaş-dövlət münasibətlərindəki "sosial inam indeksi"nin sabitliyini təmin edən strateji resursdur.

Süni İntellekt və idarəetmənin gələcəyi

1. Sİ riskləri "hüquqlar əsaslı fərdi zərər" və "sistemli-struktur zərər" spektrinə ayrılır. Mövcud tənzimləmə mexanizmləri sistemli təhdidlər qarşısında institusional acizlik nümayiş etdirdiyindən, məsuliyyət məsələsi zərərin miqyası ilə tənzimləmə alətlərinin mütənasibliyi üzərində qurulmalıdır.

2. Sİ-in idarəetməyə inteqrasiyası icraedici hakimiyyətə "analitik üstünlük" qazandıraraq hakimiyyət bölgüsü balansını dəyişir. Azərbaycanın "yuxarıdan-aşağıya" idarəetmə modeli operativ müdafiə zərurəti ilə demokratik nəzarət arasında strateji balans nöqtəsi kimi qiymətləndirilir.

Strateji ölçmə və proaktiv müdafiə modelləri

1. Dövlətin strateji dözümlülüyü infrastruktura, hüquqi bazaya, innovasiyaya və insan kapitalına əsaslanan multidissiplinar Rəqəmsal Suverenlik İndeksi (RSİ) modeli ilə əsaslandırılır.

2. Milli kibermüdafiə reaktiv yanaşmadan proaktiv "Kiber-profilaktika" paradiqmasına keçid edir. Model, təhdidləri sistemə daxil olmadan neytrallaşdıran "texniki peyvəndləmə" və strateji çəkindirməyə əsaslanan iqtisadi-siyasi səmərəsizlik prinsipləri üzərində qurulur.

Tədqiqatın **elmi yenilikləri** nəzəri-konseptual (Rəqəmsal Vestfal, alqoritmik suverenlik), metodoloji-analitik (RSİ), regional təhdid və Sİ-nin ikili məsuliyyət matrisləri), stratejidoktrinal (Sİ əsaslı monokratik icraçılıq balansı, kiberprofilaktika modeli), koqnitiv-sosial (idrakı immunitet, OODA dövrəsinin müdafiəsi) və praktiki-tətbiqi (Azərbaycanın kibertranzit imkanları, hibrid dövlət modeli) istiqamətləri ilə milli təhlükəsizlik arxitekturasının rəqəmsal paradiqmasını formalaşdırır.

Kibertəhlükəsizliyin konseptual və nəzəri çərçivəsi üzrə

1. Klassik Vestfalya sistemindən "Rəqəmsal Vestfal" modelinə keçid konseptuallaşdırılaraq, dövlət suverenliyinin "alqoritmik" və "daşınan" paradiqmaları ilk dəfə əsaslandırılmışdır. Sübut edilmişdir ki, müasir dövlət hüdudları təkcə coğrafi koordinatlarla deyil, alqoritmik nəzarət və data-yurisdiksiyası vasitəsilə müəyyən edilir.

2. L.Kellonun kibernəzəriyyələri kontekstində “alqoritmik” və “daşınan suverenlik” anlayışları ilk dəfə Azərbaycanın milli təhlükəsizlik doktrinasına inteqrasiya edilərək, dövlətin funksional varlığının həm coğrafi ərazi bütövlüyü, həm də xarici yurisdiksiyalarda qorunan kritik verilənlərlə təmin olunması əsaslandırılmışdır. Bununla da beynəlxalq hüquqda suverenliyin bölünməzliyi prinsipinə “bulud vahidi” kontekstində konseptual yanaşma irəli sürülmüşdür.

3. DIME modelinin rəqəmsal transformasiyasında “koqnitiv sahədə ortaq həqiqəti müdafiə etmək” bacarığı milli gücün komponenti kimi identifikasiya edilərək elmi dövriyyəyə daxil edilmişdir. Azərbaycanın “sahibkar” və “tənzimləyici” funksiyalarını sintez edən aktiv hibrid dövlət modeli ilk dəfə empirik təsnif olunmuşdur.

4. Milli rəqəmsal ekosistemin idarə olunmasında mütləq suverenliklə beynəlxalq məlumat dövriyyəsi arasında strateji balans yaradan “Hibrid lokallaşdırma” idarəetmə modeli milli təhlükəsizlik prioriteti kimi əsaslandırılmışdır.

5. Qlobal internet arxitekturasında rəqəmsal parçalanmanın innovasiya gücünə və milli suverenliyə mənfi təsirləri proteksionizm, texniki uyğunsuzluq və normativ fərqlilik faktorları üzrə vahid analitik çərçivədə sistemləşdirilmişdir.

Geosiyasət, regional dinamikalar və dövlət siyasəti üzrə

1. Regional təhlükəsizlik kompleksində aktorların kiberfəaliyyət motivləri sistemləşdirilmiş, Rusiyanın “total rəqəmsal müharibə” və İranın modellərinin “daimi asimmetrik sabotaj” profilləri üzərindən hibrid təhdidlərin proqnozlaşdırılmasına matris işlənmiş, Azərbaycanın kibermüdafiə arxitekturasında regional doktrinal mənşəli təhdidlərin proqnozlaşdırılması imkanları əsaslandırılmışdır.

2. Azərbaycanın geosiyasi mövqeyi ilk dəfə “kibertranzit suverenliyi” paradiqmasında tədqiq edilmiş, klassik tranzit hüququnun məlumat yurisdiksiyası ilə sintezi əsasında ölkə ərazisindən keçən verilənlər axını üzərində hüquqi və təhlükəsizlik nəzarəti mexanizmləri əsaslandırılmışdır. Sübut olunmuşdur ki, “Rəqəmsal İpək Yolu” layihəsi Azərbaycana regionda kiberstandartları diktə edən “normativ güc” statusu qazandırır və rəqəmsal konnektivliyi milli gücün fundamental komponentinə çevirir.

3. Dövlətlərin rəqəmsal məkanda texnoloji asılılığını minimallaşdırmaq və strateji dözümlülüyünü ölçmək üçün infrastruktur, hüquq, innovasiya, insan kapitalından ibarət multidissiplinar "RSİ" modeli hazırlanmış, infrastrukturun kəmiyyət və kiberdözümlülüyün operativlik göstəricilərinin sinerjisi əsasında dövlətin rəqəmsal gücünün ölçülməsi metodologiyası təklif edilmişdir.

4. Regional rəqəmsal layihələrin mahiyyəti ilk dəfə iqtisadi müstəvidən strateji-siyasi müstəviyə keçid kontekstində tədqiq edilərək, onların dövlətin "strateji muxtariyyətini" təmin edən kiberdiplomatiya aləti və "RSİ"-nin əsas metriki olduğu sübut olunmuşdur. Regional təhdidlərin təsnifatı ilə spesifik texnoloji və hüquqi preventiv mexanizmləri ehtiva edən "Strateji Müdafiə Matrisi" işlənib hazırlanmış və bunun milli təhlükəsizlik sisteminə inteqrasiyası əsaslandırılmışdır.

Sosial-koqnitiv aspektlər və idraki dözümlülük üzrə

1. R.Cervis, J.Roozenbeek və S.Van der Lindenin konseptual modelləri əsasında kibermaarifləndirmə prosesi milli təhlükəsizliyin idraki müdafiə xətti kimi əsaslandırılmış, asimmetrik təhdidlərə qarşı manipulyasiyanı bloklayan "strateji filtr" mexanizmi və Koqnitiv strateji müdafiə doktrinası işlənib hazırlanmışdır.

2. Sosial mühəndislik alətləri ilə icra edilən "Saxta Bayraq" əməliyyatlarının dövlətin strateji qərarvermə mexanizmini məhz "Səmtlənmə" mərhələsində manipulyasiya etdiyi sübut olunmuş, texniki atributasiya probleminin həlli üçün ilk dəfə "koqnitiv atributasiya" metodologiyası təklif edilmiş və kiberhücumların texniki sabotaj deyil, strateji yanlış qavrayış yaradan və xarici siyasət seçimlərini məhdudlaşdıran hibrid alət olduğu əsaslandırılmışdır.

3. Kibertəhlükəsizlik dövlətin siyasi legitimliyini və vətəndaş-dövlət münasibətlərindəki sosial inam indeksini təmin edən fundamental strateji element kimi identifikasiya edilmişdir.

Süni İntellekt, idarəetmə və gələcək çağırışlar üzrə

1. Süni intellektin qərar qəbuletməyə inteqrasiyasının icraedici hakimiyyətə "məlumat asimmetriyası" və "analitik üstünlük" qazandırdığı, bununla da hakimiyyət bölgüsünü dəyişdiyi sübut edilmişdir. Müəyyən edilmişdir ki, AR-nın Sİ Strategiyasındakı "yuxarıdan-aşağıya" idarəetmə modeli, Santaniellonun "monokratik

icraçılıq" nəzəriyyəsi ilə asimmetrik təhdidlərə qarşı operativ müdafiə zərurəti arasında rasional balans kimi konseptuallaşdırılmışdır.

2. Sİ risklərinin differensial təhlili ilə ilk dəfə "Sİ-nin ikili məsuliyyət matrisi" və "tənzimləmənin effektivlik həddi" modeli irəli sürülmüşdür. Tənzimləmənin fərdi müstəvidə effektiv, sistemli-struktur səviyyədə isə məhdud olduğu sübut edilərək, məsuliyyət paradiqması "subyektiv təqsir" yanaşmasından "zərərin miqyasının tənzimləmə alətlərinə mütənasibliyi" müstəvisinə keçirilmişdir.

3. Milli rəqəmsal infrastrukturu reaktiv yanaşmadan proaktiv paradiqmaya keçirən "Kiberprofilaktika modeli" irəli sürülmüş, M.Smeetsin "əməliyyat xərcləri" nəzəriyyəsi ilə sintez əsasında, "texniki peyvəndləmə" ilə hücumun rəqib üçün səmərəsizliyi sübut edilmiş və kibermüdafiə "strateji zəka" növü kimi əsaslandırılmışdır.

Tədqiqatın nəzəri və praktiki əhəmiyyəti. Tədqiqatın nəzəri əhəmiyyəti klassik siyasi nəzəriyyələrin rəqəmsal reallıqlarla sintezi əsasında konseptual çərçivələrin irəli sürülməsindədir. İşdə "Rəqəmsal Vestfal", "Alqoritmik nəzarət" və "Daşınan suverenlik" anlayışları vasitəsilə dövlət suverenliyinin coğrafi məkandan texnoloji müstəviyə transformasiyası əsaslandırılmışdır. Milli gücün DIME modelinə "koqnitiv sahədə ortaq həqiqəti müdafiə etmək" bacarığının əlavə edilməsi milli təhlükəsizlik nəzəriyyəsini zənginləşdirir. "RSİ" və "Sİ-nin ikili məsuliyyət matrisi" isə metodoloji innovasiya kimi əhəmiyyətlidir.

Tədqiqatın praktiki əhəmiyyəti dövlət idarəçiliyi və milli təhlükəsizlik strategiyalarının formalaşdırılması üçün təklif etdiyi alətlərlə reallaşır. Rusiya və İran modelləri əsasındakı "Regional təhdid matrisi" kiberinsidentlərin mənşəyini və sabotaj məqsədlərini öncədən müəyyənləşdirir. "Rəqəmsal İpək Yolu" çərçivəsində Azərbaycanın "kibertranzit suverenliyi" və "normativ güc" statusunun möhkəmləndirilməsi üçün mexanizmlər təqdim olunur.

Aprobasiyası və tətbiqi. Dissertasiyanın əsas elmi yenilikləri beynəlxalq və respublika miqyaslı platformalarda aprobasiya olunmuş məqalə və tezislərdə əks olunmuşdur.

Dissertasiya işinin yerinə yetirildiyi təşkilatın adı. Dissertasiya işi Azərbaycan Respublikasının Prezidenti yanında

Dövlət İdarəçilik Akademiyasının Beynəlxalq münasibətlər kafedrasında yerinə yetirilmişdir.

Dissertasiyanın struktur bölmələrinin ayrılıqda həcmi qeyd olunmaqla dissertasiyanın işarə ilə ümumi həcmi. Dissertasiya işi giriş, 4 fəsil, 11 paraqraf, 7 alt bənd, nəticə, istifadə edilmiş ədəbiyyat siyahısı və ixtisarlardan ibarətdir. Tədqiqat işinə 28 cədvəl daxildir. Giriş 12 səhifə – 21570 işarə, I fəsil 44 səhifə – 78426 işarə, II fəsil 40 səhifə – 70966 işarə, III fəsil 32 səhifə – 54982 işarə, IV fəsil 34 səhifə – 64075 işarə, nəticə 6 səhifə – 10225 işarədən ibarətdir. İstifadə edilmiş ədəbiyyat siyahısı istisna olmaqla dissertasiyanın ümumi həcmi 300244 işarədir.

İŞİN ƏSAS MƏZMUNU

Dissertasiyanın **"Giriş"** hissəsi tədqiqatın konseptual əsaslarını və elmi-metodoloji aparatını ardıcıl şəkildə formalaşdırır. Bu kontekstdə, mövzunun aktuallığı əsaslandırılmış, problemin elmi işlənmə dərəcəsi fundamental şəkildə öyrənilmiş, tədqiqatın obyekt və predmeti dəqiq diferensiasiya olunmuş, məqsəd və vəzifələr elmi yeniliyin konseptual müddəaları ilə birbaşa korrelyasiya təşkil edəcək şəkildə dəqiqləşdirilmiş, tədqiqatın nəzəri-metodoloji bazası və tətbiqi metodikası strukturlaşdırılmış, əldə olunmuş nəticələrin elmi-nəzəri əhəmiyyəti və praktiki tətbiq imkanları kompleks şəkildə öz əksini tapmışdır.

I fəsil **"Tədqiqatın konseptual, nəzəri və metodoloji əsasları"** adlanır və 4 paraqrafdan ibarətdir. "*Siyasi kontekstdə kibertəhlükəsizliyin təhlili: konseptual çərçivə və metodoloji əsaslar"* adlı 1.1. paraqrafında kiberməkan anlayışının texniki tərkibindən zühur edərək qlobal siyasətin və dövlət suverenliyinin mərkəzi elementinə çevrilməsi prosesi konseptual idarəetmə sferası kimi araşdırılmışdır. Müasir beynəlxalq münasibətlər sistemində kibergücün C.Nay və R.Keohanein klassik güc bölgüsünə uyğun "sərt" və "yumşaq" formalarının dialektik sintezi kimi təzahür etdiyi, bu sintezin milli təhlükəsizlik maraqlarını təmin edən kompleks "Kiberstrategiya" anlayışını formalaşdırdığı əsaslandırılmışdır. Paraqrafda həmçinin, rəqəmsal platformalarda BMT, NATO və Budapeşt Konvensiyası

çərçivəsində aparılan hüquqi-diplomatik tənzimləmə cəhdləri, OEWG formatındakı inklüziv müzakirələr və qlobal güclərin suveren internet layihələri fonunda yaranan rəqəmsal hegemonluq yarışının asimmetrik siyasi-strateji aspektləri kompleks şəkildə analiz edilmişdir.

1.2."Kibertəhlükəsizliyin siyasi təhlilinin metodoloji prinsipləri və aparıcı tədqiqat çərçivələri" paraqrafında kibertəhlükəsizlik sahəsindəki risklərin və dövlət strategiyalarının kəmiyyət və keyfiyyət analizi üçün tətbiq edilən multidissiplinar metodoloji arxitektura strukturlaşdırılmışdır. Tədqiqatda dövlətlərin institusional hazırlıq və daxili sabitlik səviyyələrini ölçmək məqsədilə siyasi risk analizi və strateji qiymətləndirmə metodologiyası tətbiq edilmiş, ITU-nun Qlobal Kibertəhlükəsizlik İndeksi və Belfer Mərkəzinin güc indeksi əsasında xüsusi 5 ballıq risk şkalası formalaşdırılmışdır. Aparıcı qlobal aktorların (ABŞ, Çin, Rusiya, Aİ) və Azərbaycanın milli təhlükəsizlik doktrinalarının müqayisəli keys-stadi (case-study) metodu ilə analizi həyata keçirilmiş, gələcək rəqəmsal transformasiya prosesləri üçün ssenari əsaslı proqnozlaşdırma modeli (optimist, realist və pessimist ssenarilər) vasitəsilə tədqiqatın empirik-nəzəri bazası möhkəmləndirilmişdir (cədvəl 2).

Cədvəl 2

Azərbaycanın əsas beynəlxalq kibertəhlükəsizlik indekslərindəki cari mövqeyi və dinamikası

Beynəlxalq indeks	Cari bal / səviyyə	Ölkə üzrə dinamika
ITU GCI 2024	93.76 xal (Tier 2)	+4.45 xal artım (2020-ci ilə nisbətən)

***Mənbə**: Dissertasiya işinin I fəsilində aparılan müqayisəli təhlillər əsasında müəllif tərəfindən tərtib edilmişdir.*

1.3. "*Rəqəmsal dövrün kibertəhlükəsizlik çağırışları: əsas beynəlxalq münasibətlər nəzəriyyələri kontekstində təhlil*" paraqrafında informasiya texnologiyalarının eksponensial inkişafı nəticəsində formalaşan "rəqəmsal çağ təhlükəsizliyi" fenomeni beynəlxalq münasibətlər nəzəriyyələrinin fundamental paradiqmaları prizmasından makro-səviyyədə təhlil edilmişdir. Rəqəmsallaşma dalğasının klassik coğrafi və hərbi sferaları aşaraq gücün proyeksiyasını fiziki məkandan virtual platformalara daşıdığı və dövlətlərarası qarşılıqlı əlaqələrin sürətini köklü şəkildə dəyişdirdiyi qeyd olunmuşdur. Bu virtual mühitdə yaranan

asimmetriya, anonimlik və hüquqi boşluqların ənənəvi təhlükəsizlik paradiqmalarını qismən transformasiyaya uğratdığı nümayiş etdirilərək, kibermühitin müasir çağırışlarını bütövlüklə izah etmək üçün fərqli elmi yanaşmaların (Realizm, Liberalizm, Konstruktivizm, Rollar və Kiber İttifaq nəzəriyyələri) hibrid və multidissiplinar şəkildə tətbiqinin zəruriliyi nəzəri cəhətdən əsaslandırılmışdır.

"Realizm və neorealizm nəzəriyyələri kontekstində kibertəhlükəsizlik: güc balansı və milli maraqlar"1.3.1. altbəndində kibertəhlükəsizlik ekosistemi realizm və neorealizm nəzəriyyələrinin anarxiya, suverenlik, güc balansı və milli maraqların maksimallaşdırılması prinsipləri kontekstində araşdırılmışdır. Neorealist baxış bucağından qlobal tənzimləyici ali hakimiyyətin yoxluğu dövlətləri kiberməkanı beşinci döyüş poliqonu və çəkindirmə arenası kimi qəbul etməyə sövq etdiyi, dövlətlərin texnoloji asılılığı minimuma endirmək üçün "kibersuverenlik" və hibrid müharibə strategiyalarını mənimsədikləri göstərilmişdir. Bununla belə, kiberməkanın çoxaktorlu strukturu, atribuasiya problemi və asimmetrik təbiəti fonunda klassik dövlət mərkəzli realist güc modelinin bu sahədə qismən natamam qaldığı və fərdi-rasional aktorların təsirini nəzərə alan tamamlayıcı konseptual çərçivələrə ehtiyac duyulduğu müəyyən edilmişdir.

"Liberalizm və neoliberal institusionalizm prizmasından kibertəhlükəsizlik: qlobal idarəetmə və beynəlxalq əməkdaşlıq" 1.3.2. altbəndində kiberməkanın qlobal təhlükəsizlik arxitekturası liberalizm və neoliberal institusionalizm nəzəriyyələrinin fundamental müddəaları qarşılıqlı asılılıq, kollektiv təhlükəsizlik, beynəlxalq təşkilatlar və hüquqi tənzimləmə mexanizmləri kontekstində araşdırılmışdır. Neoliberal yanaşma çərçivəsində rəqəmsal təhdidlərin transsərhəd və asimmetrik təbiətinin dövlətləri mütləq qazanc naminə unilateral siyasətdən imtina etməyə və Budapeşt Konvensiyası, NATO-nun Kibermüdafiə üzrə Birgə Mükəmməllik Mərkəzi kimi çoxtərəfli əməkdaşlıq platformalarına inteqrasiya olunmağa sövq etdiyi əsaslandırılmışdır. - Bununla belə, qlobal güclər arasındakı kəskin geosiyasi rəqabətin, informasiya asimmetriyasının və internet ekosistemindəki mülki-özəl sektor sinerjisinin yaranmasının beynəlxalq hüquqi institutların effektiv tənzimləmə qabiliyyətini məhdudlaşdırdığı və liberal əməkdaşlıq modelində müəyyən institusional böhranlar yaratdığı təhlil olunmuşdur.

"Konstruktivizm: kimlik və kibertəhdidlərin sosial inşası" 1.3.3. alt bəndində kibertəhlükəsizlik ekosistemi konstruktivizm nəzəriyyəsi və Kopenhagen məktəbinin "təhlükəsizikləşdirmə" konsepsiyası prizmasından analiz edilərək, kibertəhdidlərin sadəcə obyektiv-texniki reallıq deyil, həm də strateji diskurs, identiklik və intersubyektiv subyektiv qavrayışların məhsulu olan sosial konstruksiyalar olduğu nümayiş etdirilmişdir. Siyasi aktorların kiberməkandakı çağırışları "ekzistensial təhlükə" olaraq formalaşdırmaqla fövqəladə idarəetmə qərarlarını, məlumat millətçiliyini və sərt tənzimləmə mexanizmlərini cəmiyyət nəzdində necə legitimləşdirdiyi diskursiv analiz metodları ilə şərh olunmuşdur. Tədqiqatda dövlətlərin beynəlxalq sistemdə mənimsədikləri strateji rolların onların kibertəhlükəsizlik siyasətlərini və normativ davranış modellərini birbaşa şərtləndirdiyi elmi cəhətdən əsaslandırılmışdır.

"Mikro-Kiber İttifaqlar və kibertəhlükəsizliyə yeni nəzəri-siyasi yanaşmalar" 1.4. paraqrafında müasir dövrün geopolitik reallıqlarına uyğun "Mikro-Kiber İttifaqlar" konsepti və kibertəhlükəsizliyə dair yeni nəzəri-siyasi yanaşmalar təqdim edilərək, fəslin ümumi nəticələri formalaşdırılır. Tədqiqatda ənənəvi hərbi ittifaqların bürokratik ləngliyi ilə müqayisədə, mikro-kiber alyansların real vaxt rejimində kəşfiyyat mübadiləsinə, özəl sektor subyektləri ilə funksional sinerjiyə və konkret təhdidlərə qarşı çevik *"ad-hoc"* əməkdaşlığa imkan verən strateji strukturu elmi əsaslarla strukturlaşdırılmışdır. Nəzəriyyə kibertəhlükəsizliyin yalnız texnoloji aspekt daşımadığına dair mövcud elmi yanaşmaları inkişaf etdirərək, onu rəqəmsal dövrdə dövlət suverenliyi və milli təhlükəsizliyin mərkəzi sütunu kimi yeni sistemli konseptual çərçivədə əsaslandırır.

II fəsil **"Kibertəhlükəsizliyin siyasi ölçüləri: geosiyasət, münaqişələr və dövlət siyasəti"** adlanır və 3 paraqrafı əhatə edir.

"Qeyri-kinetik müharibələr: geosiyasi rəqabətin rəqəmsal ölçüləri" adlı 2.1. paraqrafında müasir müharibələrin xarakterinin fiziki məkandan rəqəmsal və koqnitiv sferalara transformasiyası prosesi, "qeyri-kinetik müharibə" fenomeni kontekstində makro-siyasi analiz edilmişdir. Elektron müharibə, informasiya müharibəsi və kibermüharibə sistemlərinin kəsişməsində formalaşan hibrid təhdidlər şəbəkəsi araşdırılaraq, elektromaqnit spektrinin idarə olunmasının və

asimmetrik kiberəməliyyatların müasir geosiyasi rəqabətdə aparıcı hərbi-strateji rıçaqa çevrildiyi əsaslandırılmışdır (cədvəl 3, cədvəl 4).

Cədvəl 3

Qeyri-kinetik sahələrin müqayisəli matrisi

Sahə	Mübarizə müstəvisi	Əsas təsir mexanizmi	Strateji məqsəd
Kiber	Rəqəmsal şəbəkələr	Zərərli proqramlar (APT)	Sistemin çökməsi
İnformasiya	Psixoloji/ sosial	Dezinformasiya və təbliğat	İctimai rəyin idarəedilməsi
Elektron	Elektro-maqnit spektr	Siqnal boğma (Jamming)	Texniki izolyasiya
İdarəetmə (C2)	Strateji ierarxiya	Müdaxilə və manipulyasiya	Qərarvermənin iflici

Cədvəl 4

Qeyri-kinetik müharibənin kəsişən sahələri

Sahə	Əsas xüsusiyyətlər	Nümunə aktorlar	Nümunə əməliyyatlar
Kiber müharibə	Şəbəkələrə, infrastruktura rəqəmsal hücumlar	Dövlətlər, APT-lər, haktivistlər	Ransomware, enerji şəbəkəsinə hücumlar
İnformasiya müharibəsi	İnformasiyanın, ictimai rəyin manipulyasiyası	Dövlətlər, troll fermaları, botlar	Dezinformasiya, təbliğat
Elektron müharibə	Elektromaqnit spektrinin pozulması	Hərbçilər, kəşfiyyat	Siqnal boğma, EMP hücumları
Komanda və idarəetmə müharibəsi	Qərar qəbul etmə sistemlərinin hədəf alınması	Dövlətlər	C2 sistemlərinin sındırılması

Mənbə: *Cədvəllər dissertasiya işinin II fəslində aparılan müqayisəli təhlillər əsasında müəllif tərəfindən tərtib edilmişdir.*

"Kibermüharibənin geosiyasi hərəkətverici qüvvələri və regional dinamikalar" paraqrafında müasir beynəlxalq münasibətlər sistemində dövlətlərin gücünün fiziki ərazilərin hüdudlarını aşaraq, rəqəmsal şəbəkələrin və məlumat axınlarının idarə olunması qabiliyyəti, yəni

“alqoritmik suverenlik” ilə ölçülən yeni bir mərhələyə qədəm qoyması prosesi makro-siyasi müstəvidə analiz edilmişdir. Tədqiqatda kiberməkanın dövlətlərə təmin etdiyi strateji asimmetriya, anonimlik və məsafəsizlik imkanlarının güc tətbiqinin konvensional modeldən Qeyri-Kinetik Müharibə və “Boz zona” əməliyyatlarına keçidini necə şərtləndirdiyi əsaslandırılmışdır. Bu kontekstdə Rusiyanın “Yeni Nəsil Müharibə” doktrinası və Təkmilləşdirilmiş Davamlı Təhdidlər vasitəsilə həyata keçirilən gizli infiltrasiya, “Living off the Land” texnikası, “Golden SAML” üsulları və kiber-fiziki sabotaj mərhələlərinin əməliyyat mexanizmləri strukturlaşdırılmışdır.

Paraqrafda kibermünaqişələrin regional xüsusiyyətləri xüsusi modellər üzrə təsnif edilmişdir: Asiya-Sakit okean modelində ABŞ və Çin arasındakı strateji rəqabətin “Kod müharibəsi”nə, texno-millətçiliyə və şəbəkənin fraqmentasiyasına transformasiyası, o cümlədən yarımkeçirici hegemonluğu uğrunda mübarizə və “Volt Typhoon” kimi strateji şəbəkələrdə öncədən mövqe tutma metodologiyaları təhlil olunmuşdur. Yaxın Şərq modelində enerji infrastrukturunun və SCADA sistemlərinin hədəfə alınması (Stuxnet, Shamoon keysləri), Şərqi Avropa modelində isə kiberzərbələrin kinetik hərbi əməliyyatlarla sinxronlaşdırılması (Ukrayna təcrübəsi və İT Ordusu) elmi-empirik süzgəcdən keçirilmişdir. “Rusiya modeli” (total kiber-fiziki müharibə) ilə asimmetrik “İran modeli” (proksilər vasitəsilə daimi sabotaj) qarşılaşdırılaraq, onların strateji məqsəd, texniki icra və hədəf sahələri üzrə fundamental fərqlilikləri matrisləşdirilmişdir.

Tədqiqatda regional təhdid vektorlarının kəsişməsində yerləşən, mürəkkəb geosiyasi arxitekturaya və kritik enerji infrastrukturuna malik olan Azərbaycan üçün bu modellərdən çıxacaq dərslər milli təhlükəsizlik kontekstində ümumiləşdirilmişdir. Müəllif tərəfindən əsaslandırılmışdır ki, ölkənin reaktiv müdafiədən proaktiv çəkindirməyə əsaslanan və L.Kello ilə M.Smeetsin nəzəriyyələri (Virtual silah, Suverenlik boşluğu, Əməliyyat xərcləri tezisləri) işığında formalaşan unikal “Kiber-Profilaktika Modeli”nə keçidi qaçılmaz bir imperativdir. Bu model çərçivəsində Azərbaycanın strateji qovşaqlarının (TANAP, Bakı Limanı və s.) hibrid müdafiəsi, “Suveren Bulud” və “Rəqəmsal Səfirlik” infrastrukturu vasitəsilə fiziki məkandan asılı olmayan “daşınan suverenliyin” (yaradılması, Sİ əsaslı atributiv

analitika və Deepfake detektorlarının tətbiqi, eləcə də "Rəqəmsal İpək Yolu" layihəsi ilə regional "kibertranzit suverenliyinin" əldə edilməsi dövlətin milli maraqlarını qoruyan strateji sütunlar kimi irəli sürülmüş və sistemləşdirilmişdir (cədvəl 5).

Cədvəl 5

Azərbaycan üçün strateji müdafiə matrisi

Təhdid sahəsi	Model	Profilaktik tədbir	Strateji hədəf
Enerji və logistika	Rusiya (kiber-kinetik)	Redundant (yedəklənmiş) oflayn sistemlər	Sabotajın təsirini sıfırlamaq
Dövlət məlumatları	Şərqi Asiya (TDT)	Suveren bulud infrastrukturu	Rəqəmsal suverenliyi qorumaq
Sosial sabitlik	İran/Rusiya (dezinformasiya)	AI əsaslı Deepfake detektorları	Milli birliyi qorumaq
Maliyyə sektoru	İran (sabotaj)	Kross-sərhəd kiber-sığorta planı	İqtisadi şoku azaltmaq

Mənbə: *Dissertasiya işinin II fəsilində aparılan tədqiqatlar və müəllif tərəfindən işlənib hazırlanmış "Kiber-Profilaktika Modeli" əsasında tərtib edilmişdir.*

"*Milli kibertəhlükəsizlik siyasəti: rəqəmsal suverenlik və beynəlxalq əməkdaşlıq çərçivələri*" adlı 3-cü paraqrafında Lewisə görə, kiberdiplomatiya müasir xarici siyasətin mərkəzinə keçmişdir və dövlətin rəqəmsal suverenliyi onun beynəlxalq koalisiyalardakı iştirak və təsir səviyyəsi ilə birbaşa mütənasibdir. Regional əməkdaşlıq platformaları orta güclü dövlətlərə rəqəmsal tranzit dəhlizləri üzərində nəzarət mexanizmləri vasitəsilə strateji muxtariyyət qazanmaq imkanı yaradır. Bu konseptual yanaşma Azərbaycan Respublikasının təşəbbüskarı olduğu "Digital Hub" və Trans-Xəzər Fiber-Optik Kabel layihələrinin geo-iqtisadi və geosiyasi çəkisini elmi cəhətdən əsaslandırır. Beləliklə, Azərbaycan regional rəqəmsal təhlükəsizlik arxitekturasını formalaşdıran, rəqəmsal İpək Yolunun təhlükəsizliyini təmin edən və öz strateji muxtariyyətini qoruyan mərkəzi regional aktor kimi xarakterizə olunur.

Paraqrafda təhlil edilən müqayisəli idarəetmə modelləri və qlobal təşəbbüslər sübut edir ki, rəqəmsal suverenlik dövlətin geosiyasi sağqalma strategiyasının mərkəzi sütunudur. Milli kibertəhlükə-

sizlik siyasəti və rəqəmsal suverenlik arasındakı qarşılıqlı əlaqə sürətlə təkamül edən mürəkkəb bir simbiozdur. Kibertəhlükəsizlik tədbirləri daxili rəqəmsal infrastrukturu qorumaq üçün həlledici olsa da, eyni zamanda qlobal internetin açıqlığı və transsərhəd məlumat axınları qarşısında müəyyən normativ baryerlər yaradır. Bu dialektik ziddiyyətin həlli milli muxtariyyəti kollektiv təhlükəsizlik ehtiyacları ilə tarazlaşdıran adaptiv idarəetmə çərçivələrindən keçir. Dövlətlər kibertəhdidlərin destruktiv təsirlərini minimallaşdırmaq üçün reaktiv müdafiə yanaşmasından imtina etməli, "bütöv millət" doktrinasını mənimsəməli və beynəlxalq səviyyədə kiberdiplomatiya fəaliyyətlərini gücləndirməlidirlər.

Tədqiqatın bu mərhələsində əldə olunmuş nəticələr əsasında, gələcək strateji fəaliyyət və milli siyasət uyğunluğunun obyektiv qiymətləndirilməsi üçün aşağıdakı prioritet istiqamətlər müəyyən edilmişdir:

1. Dövlətlərin rəqəmsal dözümlülük səviyyəsini ölçən RSİ-nin vahid və standartlaşdırılmış metriklərinin işlənilməsi;

2. Sİ və 5G/6G texnologiyalarının şəbəkə açıqlığına və qlobal inteqrasiyaya xələl gətirmədən milli kibermüdafiə sistemlərinə proaktiv adaptasiyası;

3. Sərhədlərarası hüquqi boşluqları dolduracaq və transmillət məlumat axınını milli suverenlik prinsipləri daxilində tənzimləyəcək beynəlxalq çoxtərəfli konvensiyaların yenilənməsi.

Rəqəmsal suverenlik mütləq mənada dövlətin daxili təhlükəsizlik və müstəqilliyini təmin etsə də, onun qlobal miqyasda "Splinternet" fenomeninə və qlobal rəqəmsal ortaq sahələrin (digital commons) aşınmasına yol açması kimi fəsadları da qaçılmazdır. Lakin vurğulanmalıdır ki, istənilən mürəkkəb rəqəmsal arxitekturanın, texnoloji sipərin və kiberdiplomatik razılaşmanın effektivliyi, nəticədə həmin sistemləri idarə edən və onlardan istifadə edən insan amilindən asılıdır. Texnoloji və hüquqi sədlər nə qədər mükəmməl təşkil olunsa da, kibertəhlükəsizliyin ən zəif və həssas həlqəsi hər zaman sosial-davranış faktorları olaraq qalmaqdadır. Bu metodoloji zərurətdən irəli gələrək, dissertasiya işinin növbəti fəslində rəqəmsal suverenliyin və kibermüdafiənin "insan ölçüsü" təhlil ediləcək, texniki müdafiə sədlərini asanlıqla manipulyasiya

etməyə qadir olan sosial mühəndislik təhdidləri və onların psixoloji-siyasi aspektləri fərdi və institusional səviyyədə tədqiq olunacaqdır.

Bu fəsildə aparılan tədqiqatlar nəticəsində aşağıdakı elmi tapıntılar əldə edilmişdir:

Sülh ilə müharibə arasındakı klassik Vestfaliya sərhədlərinin silinməsi rəqəmsal kontekstdə əsaslandırılmışdır. Estoniya (2007) və Stuxnet (2010) keysləri formal-hüquqi baxımdan müharibə sayılmasa da, strateji-siyasi nəticələrinə görə dövlət suverenliyinə qarşı birbaşa rəqəmsal təcavüz aktları kimi kiberrealizm çərçivəsində interpretasiya olunmuşdur.

Elektronik sabotaj, informasiya əməliyyatları və koqnitiv təsir komponentlərinin sintezi strukturlaşdırılmışdır. Bu modelin kinetik güclə müqayisədə minimal xərclə və atribuasiya çətinliyi fonunda siyasi hədəflərə daha proaktiv və hədəfəyönümlü və sürətli nail olmaq imkanı tanıdığı müəyyən edilmişdir.

Qlobal güclərin subyektiv maraqlarına əsaslanan üç təməl xətt (Aİ-nin "suveren açıqlıq", ABŞ-ın "liberal-şəbəkə" və Rusiya/Çinin dövlət mərkəzli "kiberavtoritarizm" modelləri) qarşılaşdırılmışdır. Bu kontekstdə dövlətlərin rəqəmsal dözümlülüyünü qiymətləndirmək üçün dördfaktorlu RSİ təklif edilmişdir.

Azərbaycan Respublika daxili hibrid müdafiə arxitekturasını formalaşdıraraq regional çərçivəni aşmış və aktiv "normativ güc" statusuna keçmişdir. Ölkənin "Rəqəmsal İpək Yolu"ndakı rolu, BMT-nin Kibercinayətkarlıq Konvensiyasını ilk ratifikasiya edənlərdən olması və NCSI reytinqində 31-ci yerə yüksəlməsi onun regionda standartları diktə edən aparıcı geosiyasi aktora çevrildiyini empirik əsaslandırır.

Yekun olaraq, qlobal rəqəmsal transformasiya erasında reaktiv texniki metodlar yetərsiz qiymətləndirilir. Milli kibersuverenliyin qorunması məqsədilə dövlət, cəmiyyət və özəl sektorun sinerjisini ehtiva edən "bütöv millət" doktrinasının tətbiqi texniki zərurətdən daha çox, birbaşa milli təhlükəsizliyin və geosiyasi sağqalmanın nüvəsini təşkil edir.

III fəsil **"Kibertəhlükəsizliyin sosial və insan mərkəzli aspektləri"** adlanır. 2 paraqraf və 2 altbənddən ibarətdir. *"Sosial mühəndisliyin təhlili: kibertəhlükəsizliyin davranış və psixoloji ölçüləri*

(nəzəriyyə və praktikanın vəhdətində)" paraqrafında kibertəhlükəsizlik ekosistemindəki ən həssas element olan "insan amili" və onun manipulyasiyasına yönəlmiş sosial mühəndislik mexanizmləri fənlərarası müstəvidə tədqiq edilmişdir. Dünya üzrə uğurlu kiberhücumların 75-95%-nin texnoloji boşluqlardan deyil, məhz insan psixologiyasının istismarından (*phishing, pretexting, deepfake*) qaynaqlandığı statistik göstəricilər əsasında sübut edilmişdir. Paraqrafda əsaslandırılmışdır ki, sosial mühəndislik artıq fərdi kibercinayətkarlıq hədlərini aşaraq rəqib dövlətlərin daxili sabitliyini pozan, qərar qəbul etmə mexanizmlərini iflic edən və dövlətin siyasi legitimliyinə birbaşa təhdid yaradan asimmetrik bir hərbi-strateji silaha çevrilmişdir.

"Rəqəmsal siyasətdə insan amili: sosial mühəndisliyin siyasi legitimlik və beynəlxalq təhlükəsizlik kontekstində strateji təhlili"adlı 3.1.1. altbölmədə kibertəhlükəsizliyin texnosentrik paradiqmadan insanmərkəzli modelə transformasiyası kontekstində sosial mühəndislik mexanizmlərinin siyasi legitimlik, hibrid müharibə və beynəlxalq təhlükəsizlik müstəvisindəki strateji rolu fundamental şəkildə təhlil edilmişdir. Karl Popperin "utopik sosial mühəndislik" xəbərdarlığı və Robert Cervisin "beynəlxalq siyasətdə qavrayış xətaları" konsepsiyası rəqəmsal məkana proyeksiya edilərək, kiberaktorların texniki boşluqlardan ziyada diplomatik qərarvericilərin koqnitiv zəifliklərini və inanc sistemlərini hədəf aldığı, bununla da subyektiv strateji korluq və yanlış kiberatribuasiya vasitəsilə əsassız eskalasiya riski yaratdığı əsaslandırılmışdır. Rentyer dövlətlərin rəqəmsal legitimlik layihələri, Rusiya-Ukrayna münaqişəsindəki dezinformasiya əməliyyatları, "HamsaUpdate" və "MuddyWater" keysləri, həmçinin Sİ və deepfake texnologiyalarının təhdidləri sənayeləşdirməsi fonunda milli rəqəmsal suverenliyin qorunmasının yalnız texnoloji divarlarla deyil, beynəlxalq etimad quruculuğu tədbirləri (CBMs), diplomatik kibernormaların təsisi və dövlət-cəmiyyət müstəvisində "koqnitiv davamlılığın" ("insan firewall-u") gücləndirilməsi ilə mümkün olduğu elmi-empirik əsaslarla sübut edilmişdir.

"Süni İntellekt və rəqəmsal manipulyasiya: seçki proseslərində sosial mühəndislik və siyasi legitimlik böhranı"3.1.2. alt bölməsində Tədqiqat işində Sİ və Big Data texnologiyalarının inkişafı fonunda sosial mühəndislik metodlarının fərdi hədəfləmədən kütləvi davranış

manipulyasiyasına transformasiyası və onun seçki proseslərində yaratdığı siyasi legitimlik böhranı kompleks şəkildə tədqiq edilmişdir. Maşın öyrənmə alqoritmləri və mikro-hədəfləmə üsulları vasitəsilə seçicilərin psixometrik profillərinin yaradılmasının namizədlərə 10-12% civarında strateji səmərəlilik üstünlüyü qazandırdığı, lakin eyni zamanda "informasiya köpükləri" vasitəsilə cəmiyyəti qütbləşdirərək demokratik institutları daxildən sarsıtdığı empirik əsaslarla sübut olunmuşdur. ABŞ (Cambridge Analytica), Fransa (Macron Leaks), Braziliya, Almaniya və Hindistanın seçki keyslərinin müqayisəli analizi əsasında qlobal rəqəmsal idarəetmə modellərinin trayektoriyaları müəyyənləşdirilmiş (cədvəl 6), Robert Cervisin qavrayış xətaları hipotezləri Sİ-nin seçki manipulyasiyası imkanları ilə ilk dəfə sintez edilərək dövlətlərin subyektiv "strateji korluq" riski ilə üz-üzə qaldığı əsaslandırılmisdir (cədvəl 6).

Cədvəl 6

Seçki manipulyasiyasında rəqəmsal texnologiyaların tətbiq dinamikası və dövlət idarəçiliyinə təsirləri

Seçki keysi/ Ölkə	Tətbiq olunan texnologiya və model	Statistik göstərici / səmərəlilik	Siyasi-strateji nəticəsi və legitimlik böhranı
2012 ABŞ *(B.Obama)*	Auditoriya analitikası və rəqəmsal davranış mo-delləşdirilməsi	Seçki kampaniyası nda 10-12% səmərəlilik artımı	"Tərəddüddə olan" (qərarsız) seçicilərin dəqiq hədəflənməsi ilə strateji qələbənin təmin edilməsi
2016 ABŞ (D.Tramp)	Big Data ana-litikası, "Cambridge Analytica" və OCEAN psixometrik profilləşməsi	50 milyondan çox fərdi Facebook profilinin qeyri-etik emalı	Seçicilərin qorxularına yönəlmiş fərdiləşdirilmiş manipulyasiya; demok-ratik seçki nəticələrinin dəyişdirilməsi
2017 Fransa (E.Makron)	NLP (təbii dil emalı) alqoritmləri və real vaxtlı sosial monitorinq	Milyonlarla rəqəmsal rəyin eyni anda semantik təhlili	Populist dezinformasi-yaya qarşı proaktiv müdafiə; Macron Leaks kiberəməliyyatının uğur-suzluğa düçar edilməsi

Cədvəl 6-nın ardı

2018 Braziliya (J.Bolsonaro)	Şifrələnmiş messencer (WhatsApp) botları və alqoritmik kütləvi yayım	Yüz minlərlə avtomatlaşdırılmış rəqəmsal mesaj	Fakt-yoxlama (*fact-checking*) mexanizmlərindən kənar informasiya köpüklərinin yaradılması və kütləvi rəy manipulyasiyası
2021 Almaniya (Bundestaq)	Avropa İttifaqının normativ hüquqi tənzimləmə filtrləri	GDPR (Ümumi məlumat mühafizəsi reqlamenti) standartları	Siyasi sosial mühəndislik qarşısında fundamental hüquqi baryerin təsisi; rəqəmsal məxfiliyin qorunması
2024 Hindistan (Parlament)	Generativ Sİ (Generative AI) və klonlaşdırılmış Deepfake alətləri	Siyasi kampaniyaların 80%-dən çoxunun Sİ dəstəkli olması	Reallıqla saxtakarlıq arasındakı sərhədlərin silinməsi; qlobal miqyasda texnoloji filtrasiya sistemlərinə zərurətin yaranması
Azərbaycan (Rəqəmsal Model)	G-Cloud (Hökumət Buludu), vahid seçici reyestri və mərkəzi Big Data arxitekturası	Seçki infrastrukturunun 100% rəqəmsal reyestr inteqrasiyası	"Texnosentrik" server mühafizəsi ilə "insanmərkəzli" koqnitiv qorunmanın sintezi; strateji muxtariyyət və milli immun sisteminin qurulması

Mənbə: *Cədvəl dissertasiya işinin III fəslində aparılan müqayisəli təhlillər əsasında müəllif tərəfindən tərtib edilmişdir.*

"Kibertəhlükəsizlikdə koqnitiv davamlılığın strateji təhlili: qavrayış nəzəriyyəsindən milli rəqəmsal immunitet sisteminədək" adlanan 3.2. paraqrafında müasir kibertəhlükəsizlik paradiqmasının dar texnosentrik şəbəkə mühafizəsindən insanmərkəzli "koqnitiv dayanıqlıq" modelinə keçidi və Robert Cervisin beynəlxalq siyasətdəki "yanlış qavrayış" nəzəriyyəsi işığında milli rəqəmsal immunitet sisteminin formalaşdırılması mexanizmləri kompleks şəkildə təhlil edilmişdir. İlk dəfə olaraq, Cervisin "avtomatik qavrayış tələləri" və siqnalların subyektiv interpretasiyası xətaları ilə J.Roozenbeek və S.Van der Lindenin "psixoloji peyvəndləmə"

metodologiyası müasir kibermüdafiə müs-təvisinə sintez edilmiş, simulyasiya əsaslı təlimlərin fərdlərdə hədəfə çevrilmə riskini 32.4%-dən 5%-ə endirdiyi riyazi cəhətdən əsaslandırılmışdır. Budapeşt Konvensiyasının 35-ci maddəsi (24/7 əlaqə şəbəkəsi) və NIST insidentlərə reaksiya dövrü çərçivəsində "qeyri-cəza mədəniyyətinin" institusionallaşdırılmasının idarəetmədə kiberinsidentlərin gizlədilməsi müddətini (orta hesabla 194 gün) qısaltdığı və iqtisadi itkiləri (4.5-4.9 mln. dollar) minimallaşdırdığı sübut olunmuşdur. XRİTDX-nin 2025-ci il dekabr ayı statistikası (mail.gov.az-da bloklanan zərərli daxilolmaların 40.8%-ə yüksəlməsi və kiberhücum göstəricilərinin 10.1%-nin istifadəçi müraciəti ilə aşkar edilməsi) əsasında Azərbaycanın "Kiber-Gigiyena", "Kiber Yay Məktəbləri" və "Rəqəmsal Könüllülər" layihələrinin dövlət aparatı və cəmiyyət səviyyəsində "sürü immuniteti" və proaktiv "insan sensoru" formalaşdırdığı, asimmetrik hücumlara qarşı milli təhlükəsizliyin ayrılmaz tərkib hissəsi olan vahid "Koqnitiv Müdafiə Doktrinası" yaratdığı nəzəri və empirik xarakterli mülahizələrlə müəyyən edilmişdir.

Cədvəl 7

Azərbaycanın kibermüdafiə göstəriciləri (2025)

Müdafiə Səviyyəsi	2025-ci il (Dekabr)	Dinamika və şərh
AzStateNet (Şəbəkə)	19,168,168 bloklama	Perimetr müdafiəsinin yüksək effektivliyi
E-poçt (mail.gov.az)	40.8% (2.2 mln + bloklama)	Fişinq hücumlarının 6 dəfə artımı
Sandbox (analiz)	4,191 zərərli sənəd	Mürəkkəb troyanların aşkarlanması
İstifadəçi (IOC müraciəti)	10.1%	Kibergigiyena layihəsinin uğuru

Mənbə: *Cədvəl dissertasiya işinin III fəslində aparılan müqayisəli təhlillər əsasında müəllif tərəfindən tərtib edilmişdir.*

Cədvəl 7-də paraqrafda irəli sürülən bütün nəzəri konsepsiyaları, hüquqi-praktiki instrumentləri və Azərbaycanın milli strateji hədəflərini (IOC göstəricilərinin 20%-ə çatdırılması hədəfi daxil olmaqla) vahid iyerarxiyada sistemləşdirir. Cədvəlin təhlili göstərir ki, kibermüdafiədə antropoloji amillər ön plana keçmişdir. mail.gov.az sistemində bloklamaların 40.8%-ə yüksəlməsi hücumların insan qavrayışına

yönəldiyini, IOC müraciətlərinin 10.1% təşkil etməsi isə J.Roozenbeek və S. van der Lindenin "psixoloji peyvəndləmə" konsepsiyasının praktik səmərəsini sübut edir, personal "zəif bənd" statusundan çıxaraq proaktiv "koqnitiv firewall" funksiyasını yerinə yetirir. Strateji hədəf 2026-cı ilədək bu göstəricini 20%-ə çatdırmaqla kollektiv "sürü immuniteti"ni təmin etməkdir.

Tədqiqatın "**Kibertəhlükəsizlikdə Süni İntellekt və gələcək çətinliklər**" adlanan dördüncü fəsil 2 paraqraf və 2 altbənddən ibarətdir və müasir beynəlxalq münasibətlər elminin mübahisəli mövzularından olan Sİ-in siyasi hakimiyyət üzərindəki transformativ təsirini əhatə edir.

"Kibertəhlükəsizlik və rəqəmsal nəzarətdə Süni İntellektin idarə edilməsi: dövlətin rolu və məsuliyyət dilemması" 4.1. paraqrafında Sİ dövlət idarəçiliyinə və kibermüdafiə sistemlərinə inteqrasiyasının hakimiyyətin təbiəti haqqında doğurduğu fundamental siyasi suallar və tənzimləmə böhranları araşdırılmışdır. Sİ-nin qərar qəbulu mexanizmlərinə daxil edilməsinin icraedici hakimiyyətə qazandırdığı "məlumat asimmetriyası" və "analitik üstünlük" nəticəsində qanunvericilik, məhkəmə və media nəzarətinin alqoritmlərin işləmə sürətindən geridə qalması prosesi tədqiqatda "analitik iflic" sindromu kimi xarakterizə olunmuşdur. M.Santaniellonun nəzəriyyəsinə tənqidi istinadən əsaslandırılmışdır ki, Sİ həm avtoritar, həm də demokratik sistemlərdə gücü icraedici orqanda cəmləşdirərək "monokratik icraçılıq" riski yaradır. Bu struktur risklərin neytrallaşdırılması üçün müəllif tərəfindən orijinal "ikili məsuliyyət matrisi" irəli sürülmüşdür; tənzimləmənin effektivliyi və zərərin miqyası oxları üzərində qurulan bu matris vasitəsilə sübut edilmişdir ki, *deepfake* seçki manipulyasiyaları və kritik infrastruktura hücumlar kimi "sistemli zərər-aşağı tənzimləmə" zonasında yerləşən kibertəhdidlər qarşısında mövcud beynəlxalq hüquqi çərçivələr (GDPR, NIS2, Budapeşt Konvensiyası) institusional acizlik nümayiş etdirir və məsuliyyətin diffuziyası problemi tənzimləmə asimmetri-yasını dərinləşdirir.

4.2."*Süni İntellekt və Kibertəhlükəsizliyin siyasi-etik ölçüləri: muxtar sistemlər və beynəlxalq təhlükəsizliyin transformasiyası*" paraqrafında Sİ və kibertəhlükəsizliyin kəsişməsində formalaşan

siyasi-etik paradiqmalar və muxtar hərbi platformaların beynəlxalq sabitlik arxitekturasında törətdiyi qlobal transformasiyalar kompleks şəkildə təhlil edilmişdir. Sİ texnologiyalarının təhlükəsizlik sahəsindəki tətbiqinin ənənəvi hərbi-siyasi çəkindirmə paradiqmalarını köklü şəkildə dəyişdirdiyi, dövlətlərin rəqəmsal suverenlik sərhədlərini virtual sferada yenidən formalaşdırdığı elmi əsaslarla göstərilmişdir. Müəllif tərəfindən vurğulanmışdır ki, rəqəmsal suverenliyin gələcəyi alqoritmlərin sürətindən deyil, şəffaflıq, etik standartlara uyğunluq və hərbi-siyasi qərarların qəbulunda mənalı insan nəzarətinin saxlanmasından birbaşa asılıdır.

4.2.1."Etik paradiqmalar və Süni İntellektin təhlükəsizlik arxitekturasında konseptual məhdudiyyətləri" alt bəndində Sİ alqoritmlərinin milli təhlükəsizlik sistemlərinə şəffaf inteqrasiyası qarşısında duran fundamental etik və texnoloji məhdudiyyətlər tədqiq olunmuşdur. Sİ sistemlərinin malik olduğu alqoritmik qərəzlilik və daxili hesablama məntiqlərinin qeyri-şəffaflığını ifadə edən "qara qutu" probleminin dövlət səviyyəsində qərar qəbul etmə prosesində yaratdığı kəskin risklər strukturlaşdırılmışdır. Tədqiqatda eyni texnologiyanın həm müdafiə/kontrdezinformasiya, həm də hücum/kiberkəşfiyyat məqsədilə eyni dərəcədə effektiv tətbiq edilə bilməsini ifadə edən "dual-use" paradoksu elmi cəhətdən şərh olunmuş və bu paradoksun kibersilahlanma yarışını klassik silahlanma yarışından daha sürətli və beynəlxalq hüquq müstəvisində tənzimlənməsi daha çətin formaya saldığı sübuta yetirilmişdir.

4.2.2."Kibermüharibədə Süni İntellekt: muxtar sistemlər, geosiyasi təhdidlər və insan hüquqları" alt bölmədə tədqiqat çərçivəsində Muxtar Kibersilahların tətbiqinin beynəlxalq münasibətlərdə yaratdığı ekzistensial çətinliklər elmi-siyasi analizə cəlb edilmiş və "insanın dövrədən kənar" fəaliyyət göstərən sistemlərin hüquqi məsuliyyət zəncirini qıraraq təcavüzkar tərəfə siyasi məsuliyyətdən yayınma imkanı verdiyi əsaslandırılmışdır. Sübut edilmişdir ki, Sİ-nin "maşın sürəti" diplomatik böhran idarəçiliyini qabaqlayaraq nəzarətsiz eskalasiyaya yol açır, alqoritmik sistemlərin "ayrımcılıq" və "nisbətlilik" prinsiplərini tam təmin edə bilməməsi isə Beynəlxalq Humanitar Hüququ (BHH) sarsıdır. Döyüş tempinin insanın idrakı nəzarətindən sürətlənməsi, "sıfır-gün" boşluqlarının avtomatik

aşkarlanması və atributsiya böhranı kiberçəkindirmə strategiyalarını səmərəsizləşdirir, qlobal güc paylanmasında rəqəmsal bərabərsizliyi artırır. Regional kontekstdə, Azərbaycan kimi orta və kiçik güclər üçün bu "saxta bayraq" əməliyyatlarının ekzistensial risk təşkil etdiyi, rəsmi Bakının kiberməkanın tənzimlənməsində və BMT səviyyəsində norma-yaradıcılıq proseslərində aktiv iştirak maraqları əsaslandırılmışdır.

Dissertasiyanın **nəticə** bölməsi aparılan tədqiqatın nəticələrini və çıxarılan əsas məqamları yekunlaşdırır. Bu çərçivədə, bulud texnologiyaları, alqoritmik sərhəd və kibertranzit suverenliyinə əsaslanan müasir milli təhlükəsizlik arxitekturasının konseptual əsasları müəyyənləşdirilmiş, R.Cervisin qavrayış xətaları və koqnitiv inokulyasiya modellərinin sintezi əsasında "koqnitiv müdafiə doktrinası" hazırlanmışdır. Sİ-in seçki manipulyasiyalarındakı rolu və doğurduğu legitimlik böhranları qlobal keyslər kontekstində analiz edilərək, Azərbaycanda vətəndaşı manipulyasiyadan qoruyan "koqnitiv immunitet" paradiqmasının effektivliyi əsaslandırılmışdır. Sİ-nin hərbi və idarəçilik sistemlərinə inteqrasiyasının etik-hüquqi xüsusiyyətləri tədqiq olunmuş, ölkənin qlobal indekslərdə ən yüksək Tier1statusuna yüksəlməsi üçün qanunvericiliyin NIS2 və GDPR standartlarına uyğunlaşdırılması, Sİ Ombudsmanı, alqoritmik şəffaflıq reyestri, suveren bulud və TDT çərçivəsində regional CERT-in yaradılması kimi proaktiv və innovativ addımları ehtiva edən strateji tövsiyələr paketi irəli sürülmüşdür.

Dissertasiyanın əsas müddəaları iddiaçının aşağıdakı nəşrlərində öz əksini tapıb:

1. Джаббарова, К.Ф. Современные аспекты кибербезопасности в мире в контексте глобальных угроз // – Россия: Самарская область, Тольятти, Журнал «Азимут научных исследований: экономика и управление»,– 2017. Том. 6, №2 (19), – с. 323-326.
2. Джаббарова, К.Ф. Важность совершенствования механизмов организации кибербезопасности в современных условиях // – Россия: Вестник Кыргызско-Российского Славянского университета. Политология, – 2017. Том 17, № 6, – с. 164-167.

3. Джаббарова, К.Ф. Актуальные вопросы изучения и применения международного опыта по обеспечению кибербезопасности // Журнал «Противодействие терроризму». Проблемы XXI века, – 2017. №2, – с. 39-43.
4. Джаббарова, К.Ф. Важные направления и элементов государственной политики по кибербезопасности в современных условиях // – Bakı: Geostrategiya, – 2017. №02(38), – s. 74-76.
5. Джаббарова, К.Ф. Важность обеспечения кибербезопасности в мире в условиях трансформации механизмов национальной безопасности. X международной конференции «Обмен результатами исследований в рамках международного сближения ученых», – Канада, Монреаль, 7 февраля, – 2017, – с.84-89.
6. Джаббарова, К.Ф. Проблемы и пути решения кибербезопасности в мире в условиях роста киберпреступлений // – Bakı: Geostrategiya, – 2018. №01(43), – s. 70-72.
7. Jabbarova, K.F. The Important Aspects of Strengthening the Material and Technical Base of The Cybersecurity System // – USA, Philadelphia. Technology and science, International Scientific Journal Theoretical & Applied Science, – 2018, No.02, Volume 58, – pp. 154-159.
8. Jabbarova K.F. AI and Cybersecurity – New Threats and Opportunities: [Electronic resource] / Pakistan Journal of Life and Social Sciences. – 2024, Vol. 22, №2, – pp. 9966–9975.
9. Jabbarova, K. Securing the Future: Integrating AI Safety into Cybersecurity Frameworks: [Electronic resource] / Journal Edelweiss Applied Science and Technology. – 2025, Vol. 9, №8, – pp.1452–1463.
10. Cabbarova, K.F. Kibertəhlükəsizliyin Realizm və Neorealizm nəzəriyyələri kontekstində təhlili // Bakı Avrasiya Universiteti. Sivilizasiya, – 2025. №2, cild 14, – s. 58-56
11. Cabbarova, K.F. Rəqəmsal idarəetmədə kibertəhlükəsizlik və Sİ idarəetməsi: dövlətin rolu və məsuliyyət dilemması // “Dayanıqlı inkişafın milli prioritetləri: rəqabətqabiliyyətli

iqtisadiyyat, sosial ədalətə əsaslanan cəmiyyət, müasir innovasiyalar və təmiz ətraf mühit" Respublika konfransı, – Bakı Avrasiya Universiteti, – 04 dekabr, – 2025, – s.123-132.
12. Cabbarova, K.F. Qeyri-kinetik müharibələr: geosiyasi rəqabətin rəqəmsal ölçüləri // 6-cı Qarabağ Beynəlxalq Elmi Araşdırmalar Konfransı, – Şuşa, – 23-24 aprel, – 2026.

Dissertasiyanın müdafiəsi 29 iyun 2026-cı il tarixində saat 11.00-da Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyası nəzdində fəaliyyət göstərən FD 2.30 Dissertasiya şurasının iclasında keçiriləcək.

Ünvan: AZ 1001, Bakı şəhəri, Səbail rayonu, Lermontov küçəsi 74.

Dissertasiya ilə Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyasının kitabxanasında tanış olmaq mümkündür.

Avtoreferatın elektron versiyası Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyasının rəsmi internet saytında (https://dia.edu.az/) yerləşdirilmişdir.

Avtoreferat 26 may 2026-cı il tarixində zəruri ünvanlara göndərilmişdir.

Çapa imzalanıb: 24.04.2026

Kağızın formatı: A5

Həcm: 47973 işarə

Tiraj: 100