Şəbəkə-Kommunikasiya Suverenliyi: Problemlər, Təhlükəsizlik Məsələləri, Risklər və Həlli Yolları

Rəşid Ələkbərov
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
rashid.alakberov@gmail.com

***Xülasə— Müasir dövrdə şəbəkə-kommunikasiya suverenliyi dövlətlərin milli təhlükəsizliyi* və rəqəmsal inkişafı üçün strateji əhəmiyyət daşıyır. Bu məqalədə şəbəkə-kommunikasiya suverenliyinin mövcud vəziyyəti, aktual problemləri, təhdidlər, risklər və əsas komponentləri təhlil edilir. Həmçinin, milli rəqəmsal müstəqilliyin təmin olunması üçün tövsiyə olunan həll yolları təqdim olunur. Araşdırma göstərir ki, hüquqi baza, texnoloji infrastruktur, məlumat təhlükəsizliyi, kadr potensialı, iqtisadi resurslar və ictimai maarifləndirmə sahələrinin gücləndirilməsi şəbəkə-kommunikasiya suverenliyinin effektiv qorunmasını təmin edir.**

Açar sözlər— Şəbəkə-kommunikasiya suverenliyi; kiber təhlükəsizlik; milli informasiya infrastrukturu; məlumat təhlükəsizliyi; rəqəmsal suverenlik.

I. GİRİŞ

İnformasiya və kommunikasiya texnologiyaları (İKT) müasir cəmiyyətin sosial, iqtisadi və inzibati həyatında mərkəzi rol oynayır. Elektron hökumət, rəqəmsal iqtisadiyyat və sosial şəbəkələr kimi sahələrdə şəbəkə-kommunikasiya infrastrukturunun təhlükəsizliyi və suverenliyi milli təhlükəsizliyin əsas komponentlərindən biridir. Bu baxımdan, şəbəkə-kommunikasiya suverenliyi həm milli təhlükəsizliyin təmin olunmasında, həm də strateji informasiya resurslarının qorunmasında həlledici rol oynayır. Şəbəkə-kommunikasiya suverenliyi bir ölkənin internet və informasiya resursları üzərində tam nəzarət imkanını, məlumatların təhlükəsizliyini və xarici müdaxilələrdən qorunma qabiliyyətini ifadə edir.

Mövzunun aktuallığı bir neçə amillə izah olunur. Rəqəmsallaşmanın sürətli inkişafı dövlət və biznes sektorunda İKT-nin tətbiqini artırır və milli informasiya resurslarının qorunmasını zəruri edir. Qlobal səviyyədə kiberhücumlar daha mürəkkəb və hədəfli xarakter daşıyır ki, bu da milli təhlükəsizliyə birbaşa təhdid yaradır. Eyni zamanda, məlumatların xarici serverlərdə saxlanması milli informasiya suverenliyinə təzyiq göstərir və dövlətlərin strateji qərar və iqtisadi layihələr üzərində tam nəzarət imkanlarını məhdudlaşdırır.

II. ƏLAQƏLİ İŞLƏR

Məqalə [1]-də rəqəmsal suverenlik və kiber təhlükəsizlik idarəçiliyinin hüquqi təsirləri, eləcə də dövlət nəzarətinin sənaye əsaslı formalaşması təhlil olunur. Araşdırmada rəqəmsal seqmentasiya, yəni internetin parçalanması və onun qlobal informasiya mühitinə təsirləri ətraflı şəkildə analiz edilir. Məqalə [2]-də milli rəqəmsal ekosistemlərin qorunması və demərkəzləşdirmə kontekstində kiber təhdidlərə qarşı tətbiq olunan strategiyalar araşdırılır. Tədqiqatda rəqəmsal suverenlik milli təhlükəsizlik prizmasından təhlil edilir. Məqalə [3]-də rəqəmsal suverenliyin nəzəri əsasları və kiberməkanda dövlət nəzarətinin ərazi sərhədlərindən kənarda necə formalaşdığı təhlil olunur. Eyni zamanda bu nəzarətin beynəlxalq hüquq, yurisdiksiya prinsipləri və məlumat azadlığı ilə uzlaşdırılması problemlərinə diqqət yetirilir. Məqalə [4]-də rəqəmsal suverenliyin mövcud konseptual modelləri sistemləşdirilir və onların dövlət nəzarəti, bazar mexanizmləri və insan hüquqları baxımından əsas xüsusiyyətləri təsvir edilir. Bundan əlavə, modellərin praktik tətbiq imkanları və zəif tərəfləri tənqidi şəkildə qiymətləndirilərək daha balanslı suverenlik yanaşmalarının zəruriliyi vurğulanır. Məqalə [5]-də kibersuverenliyin milli təhlükəsizliyin təmin olunmasında oynadığı əsas rol araşdırılır və dövlətlərin rəqəmsal məkanı qorumaq məqsədilə tətbiq etdiyi siyasət və tənzimləmə mexanizmləri təhlil edilir. Həmçinin kiber təhdidlərin qarşısının alınmasında hüquqi çərçivələrin və institusional idarəetmənin əhəmiyyəti ön plana çəkilir. Məqalə [6]-da beynəlxalq hüquq müstəvisində rəqəmsal sərhədlər anlayışı təhlil edilərək kiber təhlükəsizlik və rəqəmsal suverenlik sahəsində mövcud normativ boşluqlar müəyyənləşdirilir. Tədqiqat bu boşluqların aradan qaldırılması üçün dövlətlərin hüquqi öhdəliklərini, beynəlxalq əməkdaşlığın rolunu və yeni normativ yanaşmaların formalaşdırılmasının vacibliyini əsaslandırır. Məqalə [7]-də Avropa Birliyinin NIS2 Direktivinin nümunəsində rəqəmsal suverenliyin praktik səviyyədə necə reallaşdırıldığı araşdırılır. Tədqiqat çərçivəsində dövlət və özəl sektor üçün kibertəhlükəsizlik öhdəlikləri, risklərin idarə olunması mexanizmləri, insidentlərin bildirilməsi tələbləri və milli nəzarət orqanlarının rolu təhlil olunur. Məqalə [8]-də Çinin kibersuverenlik yanaşması nümunə kimi təhlil edilərək kiberməkanda dövlət dominantlığının nəzəri cəhətdən mümkünlüyü qiymətləndirilir. Araşdırmada kiber təhlükəsizlik strategiyaları, informasiya nəzarəti mexanizmləri və bu modelin qlobal internet idarəçiliyinə potensial təsirləri müzakirə olunur.

III. ŞƏBƏKƏ-KOMMUNİKASİYA SUVERENLİYİNİN KONSEPTUAL MODELİ VƏ KOMPONENTLƏRİ

Şəbəkə-kommunikasiya suverenliyi, dövlətin rəqəmsal kommunikasiya infrastrukturuna, məlumat axınlarına və texnoloji standartlara öz ərazisində müstəqil nəzarət imkanını ifadə edir. Konseptual baxımdan bu suverenlik modeli bir neçə əsas prinsipə əsaslanır: milli təhlükəsizlik və dövlət maraqlarının qorunması, informasiya azadlığı və innovasiya ilə balansın təmin olunması, eləcə də cəmiyyətin kibertəhlükəsizlik

DOI: 10.25045/cyber.gov.2026.03

və məlumat suverenliyi sahəsində maarifləndirilməsi. Model dövlətin texnoloji, institusional və hüquqi imkanlarının birgə işləməsi ilə milli rəqəmsal müstəqilliyi təmin etməyi hədəfləyir və qlobal internet prinsipləri ilə milli maraqlar arasında optimal balans yaratmağa yönəlib. Konseptual model həmçinin məlumat axınlarının izlənməsi və idarə olunması, kiber təhlükəsizlik, milli domen və DNS sistemi, yerli texnoloji təminat və hüquqi tənzimləmə kimi elementlərin inteqrasiyasını nəzərdə tutur (Şəkil. 1).

Şəkil 1. Rəqəmsal dövlətin şəbəkə-kommunikasiya suverenliyinin konseptual modeli

Şəbəkə-kommunikasiya suverenliyinin konseptual modeli bir neçə əsas komponentdən ibarətdir:

Milli şəbəkə infrastrukturu: Milli şəbəkə infrastrukturu ölkə daxilində internet və rabitə şəbəkələrinin qurulması və idarə olunmasını əhatə edir. Bu infrastrukturun dövlət nəzarətində olması milli informasiya axınının fasiləsizliyini təmin edir və xarici müdaxilələrdən qorunmasını gücləndirir.

İnternet trafikinin idarə olunması: İnternet trafikinin idarə olunması məlumat axınının monitorinqi, yönləndirilməsi və optimallaşdırılması vasitəsilə şəbəkə təhlükəsizliyinin təmin edilməsinə və informasiya resurslarının effektiv istifadəsinə xidmət edir.

- Rabitə təhlükəsizliyi: Rabitə təhlükəsizliyi məlumatların ötürülməsi zamanı məxfilik, bütövlük və əlçatanlıq prinsiplərinin qorunmasını təmin edir və kənar müdaxilə, məlumat sızması və manipulyasiya risklərini minimuma endirir.
- Milli data mərkəzləri: Milli data mərkəzləri dövlət və strateji əhəmiyyətli məlumatların ölkə daxilində saxlanmasını və emalını təmin edir, beləliklə informasiya suverenliyinin möhkəmləndirilməsində mühüm rol oynayır.
- Rəqəmsal asılılığın azaldılması: Rəqəmsal asılılığın azaldılması xarici platforma və texnologiyalardan istifadənin minimuma endirilməsini və yerli rəqəmsal həllərin təşviqini nəzərdə tutur, bununla da milli müstəqillik gücləndirilir.
- Milli domen və DNS sistemi: Milli domen və DNS sistemi internet resurslarının ünvanlandırılmasının dövlət nəzarətində həyata keçirilməsini təmin edir, nəticədə informasiya məkanının sabitliyi və təhlükəsizliyi artır.
- Qanunvericilik və standartlaşdırma: Qanunvericilik və standartlaşdırma şəbəkə-kommunikasiya sahəsində hüquqi tənzimləmələrin və texniki normaların müəyyən edilməsini təmin edir və milli maraqların qorunmasına xidmət edir.

IV. ŞƏBƏKƏ-KOMMUNİKASİYA SUVERENLİYİNİN PROBLEMLƏRİ, TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ VƏ RİSKLƏR

Müasir dövrdə şəbəkə–kommunikasiya suverenliyinin qorunması qloballaşma, rəqəmsallaşmanın sürətlənməsi və informasiya texnologiyalarının transsərhəd xarakter alması fonunda bir sıra mürəkkəb strateji problemlər, çoxşaxəli risklər və yeni təhlükəsizlik çağırışları ilə müşayiət olunur.

4.1 Şəbəkə-kommunikasiya suverenliyinə təhdid yaradan əsas problemlər:

- Xarici infrastruktur və provayderlərə asılılıq – İnternet magistralları, bulud xidmətləri və əsas platformalar üzrə xarici asılılıq texniki və siyasi riskləri artırır.
- Məlumat axınının xarici ölkələrdə idarə olunması – Məlumatların xarici serverlərdə saxlanması hüquqi nəzarətin zəifləməsinə və suverenlik risklərinə səbəb olur.
- Kiberhücumlar və kiberkəşfiyyat təhlükəsi – Dövlət qurumları və kritik infrastrukturun artan kiber risklərə məruz qalması təhlükəsizlik səviyyəsini zəiflədir.
- Milli internet resurslarının qorunmasında zəifliklər – Texniki və institusional çatışmazlıqlar dövlət və yerli informasiya sistemlərini hücumlara açıq edir.
- Hüquqi tənzimləmələrin yetərsizliyi – Qanunvericiliyin texnoloji inkişafdan geri qalması hüquqi boşluqlar və məsuliyyət problemləri yaradır.
- Texniki və insan resurslarının çatışmazlığı – İxtisaslı kadrların və müasir texnologiyaların məhdudluğu.

4.2. Məlumat və infrastruktur təhlükəsizliyi problemləri - Məlumat və infrastruktur təhlükəsizliyi problemləri xarici asılılıq, zəif texniki müdafiə və hüquqi boşluqlar səbəbindən milli təhlükəsizlik üçün ciddi risklər yaradır:

- Milli təhlükəsizlik – Xarici infrastruktura asılılıq, kiberkəşfiyyat və məlumat axınının xaricdə idarə olunması dövlət sirrlərinin sızması və strateji qərarların xarici təsirə məruz qalması ilə nəticələnə bilər.
- Məlumatların məxfiliyi – Şəxsi, korporativ və dövlət məlumatlarının xarici serverlərdə saxlanması icazəsiz istifadə və üçüncü tərəflərə ötürülmə riskini artırır.
- Texnoloji təhlükəsizlik – Kritik infrastrukturun və milli resursların zəif texniki müdafiəsi kiberhücumlara qarşı zəif dayanmağa səbəb olur.

- Xidmətlərin davamlılığı – Xarici provayderlərdə texniki nasazlıqlar, siyasi qərarlar və ya sanksiyalar internet və rəqəmsal xidmətlərin kəsilməsinə gətirib çıxara bilər.
- Hüquqi təhlükəsizlik – Hüquqi boşluqlar kiberhücum zamanı məsul tərəflərin müəyyən edilməsini çətinləşdirir və hüquqi müdafiəsizliyi artırır.

4.3. Şəbəkə-kommunikasiya suverenliyindəki problemlər bir sıra qarşılıqlı əlaqəli risklər yaradır ki, bunlar milli təhlükəsizlikdən iqtisadi və texnoloji asılılığa, məlumat təhlükəsizliyindən xidmətlərin fasiləsizliyinə və hüquqi çərçivəyə qədər müxtəlif sahələrdə ciddi nəticələr doğura bilir:

- Milli təhlükəsizlik riskləri – Dövlət sirrlərinin sızması, kritik sistemlərin iflic olması və xarici təsirlərin strateji qərarlara mənfi təsiri.
- Məlumat təhlükəsizliyi və rəqəmsal suverenlik riski – Məlumatların icazəsiz istifadəsi və ötürülməsi nəticəsində suverenliyin zəifləməsi və ictimai etimadın azalması.
- İqtisadi və texnoloji asılılıq riski – Xarici platforma monopoliyalarının yerli İT sektorunun inkişafını məhdudlaşdırması və maliyyə axınının ölkədən kənara yönəlməsi.
- Kibercinayətkarlıq və sabotaj riski – Zəif müdafiə mexanizmləri səbəbindən kiberhücumların artması və ciddi maliyyə–informasiya itkilərinin yaranması.

V. ŞƏBƏKƏ-KOMMUNİKASİYA SUVERENLİYİNİN PROBLEMLƏRİNİN, TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİNİN VƏ RİSKLƏRİNİN HƏLLİ YOLLARI

Müasir dövrdə şəbəkə-kommunikasiya suverenliyinin qorunması üçün qarşıya çıxan problemlərin ,təhlükəsizlik məsələlərinin həlli və risklərin azaldılması bir sıra strateji, texnoloji, hüquqi və təşkilati tədbirlərin ardıcıl həyata keçirilməsini tələb edir və bunlar aşağıdakı sahələri əhatə edir.

Problemlərin həllinin əsas yolları

- Rəqəmsal və texnoloji suverenliyin gücləndirilməsi – Milli data mərkəzləri və yerli bulud infrastrukturu vasitəsilə xarici asılılığın azaldılması və xidmətlərin fasiləsizliyinin təmin olunması.
- Məlumatların lokallaşdırılması və effektiv idarəetmə mexanizmləri – Strateji və şəxsi məlumatların ölkə daxilində saxlanması üçün hüquqi, texniki və nəzarət mexanizmlərinin gücləndirilməsi.
- Kibertəhlükəsizlik infrastrukturunun inkişafı – Milli CERT/SOC strukturlarının gücləndirilməsi və insidentlərə operativ cavab sistemlərinin yaradılması.
- Milli internet resurslarının qorunması və standartlaşdırılması – Vahid təhlükəsizlik standartlarının tətbiqi, ehtiyat nüsxələmə və bərpa mexanizmlərinin qurulması.
- Hüquqi və normativ bazanın təkmilləşdirilməsi – Kibertəhlükəsizlik və məlumatların qorunması üzrə qanunvericiliyin beynəlxalq təcrübəyə uyğun yenilənməsi.
- İnsan kapitalının və texnoloji potensialın inkişafı – Peşəkar kadr hazırlığı, sertifikasiya proqramları və institusional imkanların genişləndirilməsi.

Təhlükəsizlik məsələlərinin həllinin əsas istiqamətləri:

- Milli təhlükəsizliyin təmin edilməsi – Strateji məlumatların ölkə daxilində saxlanması və kiberhücumlara qarşı milli müdafiə infrastrukturunun gücləndirilməsi.
- Məlumatların məxfiliyinin qorunması – Məlumat axınına nəzarət, sertifikatlaşdırma və real vaxt monitorinq mexanizmlərinin tətbiqi.
- Kritik informasiya infrastrukturlarının müdafiəsi – Təhlükəsizlik standartlarının tətbiqi, ehtiyat nüsxələmə və bərpa sistemlərinin qurulması.
- Xidmətlərin fasiləsizliyinin təmin olunması – Yerli server və bulud infrastrukturu vasitəsilə xarici asılılığın azaldılması.
- Risklərin idarə olunmasının əsas istiqamətləri
- Milli təhlükəsizlik risklərinin azaldılması – Xarici infrastruktura asılılığın azaldılması, strateji məlumatların ölkə daxilində saxlanması və güclü kiber müdafiə sistemlərinin qurulması.
- Məlumat təhlükəsizliyi və rəqəmsal suverenliyin təmin edilməsi – Məlumatların lokallaşdırılması, sertifikatlaşdırma və müntəzəm audit mexanizmlərinin tətbiqi.
- İqtisadi və texnoloji asılılığın azaldılması – Yerli İT sektorunun inkişafının təşviqi, açıq mənbə texnologiyalarının tətbiqi və rəqabət mühitinin gücləndirilməsi.
- Xidmətlərin etibarlılığı və fasiləsizliyinin təmin olunması – Dayanıqlı server infrastrukturu, ehtiyat nüsxələmə və fövqəladə hallara hazırlıq mexanizmlərinin qurulması.
- Kibertəhlükəsizlik sistemlərinin gücləndirilməsi – Milli CERT/SOC strukturlarının inkişafı, real vaxt monitorinq və insidentlərə çevik cavab imkanlarının yaradılması.

NƏTİCƏ

Şəbəkə-kommunikasiya suverenliyi dövlətlərin milli təhlükəsizliyi və rəqəmsal müstəqilliyi üçün strateji əhəmiyyət daşıyır. Araşdırma göstərir ki, xarici infrastruktura asılılıq, məlumat axınının ölkə hüdudlarından kənarda idarə olunması, kiberhücumlar və hüquqi çatışmazlıqlar əsas risklər yaradır. Bu problemlərin həlli üçün məqalədə milli məlumat mərkəzlərinin yaradılması, məlumatların lokallaşdırılması, kibertəhlükəsizlik infrastrukturunun gücləndirilməsi, hüquqi və institusional bazanın təkmilləşdirilməsi, eləcə də insan kapitalının inkişafı vacib olduğu vurğulanmışdır. Belə tədbirlər rəqəmsal suverenliyi möhkəmləndirir, milli informasiya resurslarının

etibarlı idarə olunmasını təmin edir və dövlətin strateji qərarvermə imkanlarını artırır.

ƏDƏBİYYAT

[1] L.S. Krishna. “Digital Sovereignty and Cybersecurity Governance: Legal Implications of State Control in a Fragmented Internet,” Innovative Research Thoughts, 2023, 9(3), pp.199–209.
https://doi.org/10.36676/irt.v9.i3.1648

[2] I.K. Kwentoa. “Cybersecurity in Digital Sovereignty: Protecting National Digital Ecosystems against Foreign Cyber Infiltration in the Age of Decentralized Technology.” Journal of Next Generation Research 5.0. 2025. Volume 1, Issue 4, pp.1-14.
https://doi.org/10.70792/jngr5.0.v1i4.130

[3] F. Pierucci. “Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace.” Digital Society (Springer).2025, Vol. 4, article number 27, pp. 1-19.
https://doi.org/10.1007/s44206-025-00189-4

[4] S.Fratini, E.Hine, C. Novelli, H. Roberts. L. Florid. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models . Digital Society (Springer) Vol. 3, article number 59, (2024), pp.1-27.
https://doi.org/10.1007/s44206-025-00189-4

[5] N. Akhtar, A. R. Iqbal. Cyber Sovereignty: National Security in the Digital Age. Lahore Institute for Research and Analysis Journal. Vol. 3 (2025), pp. 87-104. https://doi.org/10.51846/kc3kjz12.

[6] K.Balarabe. Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law. Computer Law & Security Review (Elsevier),2025, Volume 58, page 106-180, https://doi.org/10.1016/j.clsr.2025.106180

[7] M. Kianpour, P. A. E. Davis, I.M.Windekilde. Digital sovereignty in practice: analyzing the EU’s NIS2 directive . International Journal of Information Security (Springer). 2025. Vol. 24, article number 167, pp.1-11. https://doi.org/10.1007/s10207-025-01090-4

[8] A.L.Kahraman. Is a Theory of Cyberspace Dominance Possible? An Assessment from the Perspective of China’s Cyber Sovereignty Approach. Güvenlik Stratejileri Dergisi,2024, pp. 131-149. DOI: 10.17752/guvenlikstrtj

Network-Communication Sovereignty: Issues, Security Challenges, Risks, and Solutions

Rashid Alakbarov

Institute of Information Technology, Baku, Azerbaijan

Abstract– In the modern era, network-communication sovereignty holds strategic importance for national security and digital development of states. This article analyzes the current state of network-communication sovereignty, its pressing issues, threats, risks, and key components. Additionally, it presents recommended solutions for ensuring national digital independence. The study demonstrates that strengthening the legal framework, technological infrastructure, information security, human resources, economic resources, and public awareness ensures the effective protection of network-communication sovereignty.

Keywords– Network-communication sovereignty, cybersecurity, national information infrastructure, information security, digital sovereignty.