

Dövlətin Kibersuverenliyi Sahəsində Elmi Araşdırmalar: Multidissiplinar Təhlil, Trendlər və Perspektivlər

Nərmin Adıgözəlova

İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

narmin66@gmail.com

Xülasə— Son dövrlər milli təhlükəsizlik kontekstində kibertəhlükəsizlik və kibersuverenliyin əhəmiyyəti artmaqdadır. Bu artımın başlıca səbəbi dövlətlərin, kritik infrastrukturun və vətəndaşların rəqəmsal mühitdən daha çox istifadə etməsidir. Tədqiqat işində Scopus və Web of Science elmi bazalarında “Cyber Sovereignty” istiqamətində aparılmış tədqiqatlar təhlil edilmiş və dərc olunan əsərlərin bibliometrik analiz aparılmışdır. Bibliometrik analiz bu sahədə çap olunan əsərlərin illər, dillər, elm sahələri və coğrafi paylanması kimi göstəricilərə əsasən aparılmışdır. O cümlədən 2015-2025-ci illər ərzində bu istiqamətdə aparılan tədqiqatların nəticələri analiz edilmiş və mövcud problemlər müəyyən edilmişdir.

Açar sözlər— kibersuverenlik; bibliometrik analiz; elmi əsərlərin analizi; beynəlxalq elmi baza.

I. Giriş

Rəqəmsallaşma proseslərinin qlobal miqyasda sürətlənməsi dövlətlərin informasiya məkanında suverenlik məsələsini prioritet istiqamətə çevirmişdir. Kibersuverenlik anlayışı dövlətin öz kiberməkanında hüquqi, texnoloji və inzibati nəzarət imkanlarını ifadə edir. Bu anlayış xüsusilə son onillikdə beynəlxalq münasibətlər, informasiya təhlükəsizliyi və rəqəmsal idarəetmə kontekstində geniş müzakirə olunur [1].

Kibersuverenlik konsepsiyası müxtəlif dövlətlər tərəfindən fərqli şəkildə şərh olunur. Məsələn, Çində kibersuverenliyi milli təhlükəsizliyin əsas elementi kimi qiymətləndirərək internet üzərində dövlət nəzarətini gücləndirməyə yönəlmiş siyasət yürüdü [2]. ABŞ-da isə daha açıq və qlobal internet modelini müdafiə edir [3]. Avropa Birliyi çərçivəsində isə rəqəmsal suverenlik anlayışı məlumatların qorunması və texnoloji müstəqillik kontekstində inkişaf etdirilir. Bu fərqli yanaşmalar elmi tədqiqatlarda da öz əksini tapır və mövzunun multidissiplinar xarakterini gücləndirir [4].

İKT-nin sürətli inkişafı və gündəlik həyatın bütün sahələrinə inteqrasiyası cəmiyyətin sosial, iqtisadi və s. strukturlarında əsaslı dəyişikliklərə səbəb olmuşdur. Bu dəyişikliklər iqtisadiyyat, təhsil, səhiyyə, nəqliyyat, dövlət idarəçiliyi və digər sahələrdə rəqəmsal sistemlərin geniş tətbiqi ilə müşayiət olunur. Beləliklə, rəqəmsal mühit imkanları artırmaqla yanaşı, bu sahələrin kibertəhlükələrə qarşı daha həssas vəziyyətə düşməsinə səbəb olmuşdur [5, 6].

İnformasiya sistemləri və rəqəmsal platformalar üzərində artan asılılıq, dövlət və cəmiyyətin kiberməkanda mövcud olan

risklərə qarşı daha həssas olmasına gətirib çıxarır. Hazırda həm dövlət, həm də özəl sektor subyektləri fəaliyyətini rəqəmsal mühit üzərindən həyata keçirdiyindən, onların kibertəhlükəsizliyinin təmin olunması strateji əhəmiyyət kəsb edir [7]. Kibertəhlükələr artıq təkə fərdi və təşkilati səviyyədə deyil, həm də milli və beynəlxalq təhlükəsizlik sistemləri üçün real təhdidlər yaradır. Bu kontekstdə kibertəhlükəsizliyin təmin olunması dövlətlər üçün prioritet məsələyə çevrilmişdir. İnformasiya sistemlərinin və şəbəkələrinin müdafiəsi, kibercinayətkarlığın və kibercasusluğun qarşısının alınması, habelə milli informasiya məkanının bütövlüyünün qorunması üçün hüquqi, texnoloji və idarəetmə baxımından kompleks tədbirlərin həyata keçirilməsi zəruridir [8,9]. Məhz bu baxımdan, kibersuverenlik anlayışı müasir dövrdə xüsusi aktualıq qazanır və milli təhlükəsizlik kontekstində əsas anlayışlardan biri kimi çıxış edir. Kibersuverenlik – dövlətin öz kiber məkanında informasiya axınlarını, rəqəmsal resursları və texnoloji infrastrukturunu müstəqil şəkildə idarə etmək, onları xarici təsir və müdaxilələrdən qorumaq qabiliyyəti kimi müəyyən olunur [10,11].

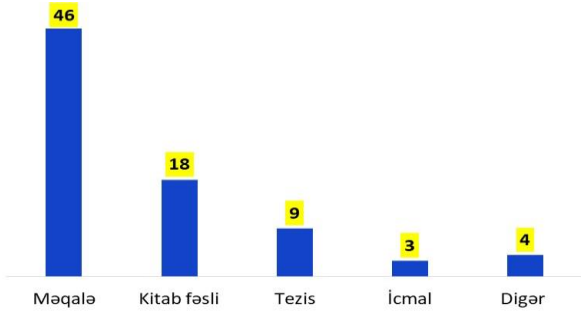
Son illər müxtəlif ölkələrdə kibersuverenliyin təmin olunması istiqamətində mövcud problemlər, perspektivlər və s. kimi bir sıra elmi-nəzəri problemlər araşdırılır və onun həlli istiqamətində yanaşmalar təklif olunur. Bu məqsədlə tədqiqat işində kibersuverenlik sahəsində mövcud olan problemlər təhlil edilmiş, müxtəlif beynəlxalq elmi bazalarda (Scopus, Web of Science və s.) indekslənmə elmi əsərlər sistemli şəkildə analiz olunmuşdur [12, 13, 14].

II. BEYNƏLXALQ ELMİ BAZALARDA KIBERSUVERENLİK ÜZRƏ NƏŞRLƏRİN ANALİZİ

Son zamanlar müxtəlif tədqiqat sahələrinin qiymətləndirilməsi və trendlərin müəyyən olunması üçün Scopus və Web of Science (WoS) kimi nüfuzlu beynəlxalq elmi bazalarının imkanlarından geniş şəkildə istifadə olunur. Bu bazalar müasir elmi fəaliyyətin təhlilində dəqiqlik təqdim etməklə, tədqiqatların sistemli şəkildə qiymətləndirilməsinə şərait yaradır. Elmi fəaliyyətin qiymətləndirilməsi, tədqiqatların təsir gücünün müəyyənəşdirilməsi və elm siyasətinin formalaşdırılması məqsədilə beynəlxalq elmi bazaların rolu əvəzsizdir.

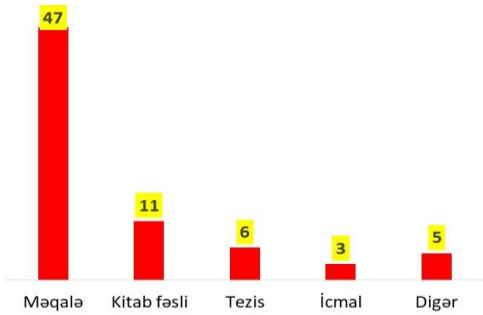
Qeyd olunan hər 2 elmi baza üzrə “Cyber Sovereignty” açar sözü üzrə axtarış etdikdə müxtəlif nəticələr əldə olunur.

Belə ki, Scopus bazası üzrə “Cyber Sovereignty” sözünü axtarıb etdikdə 80 elmi əsərin olduğunu görmək mümkündür. Bu elmi əsərlərin tipə görə paylanması Şəkil 1-də göstərilmişdir.



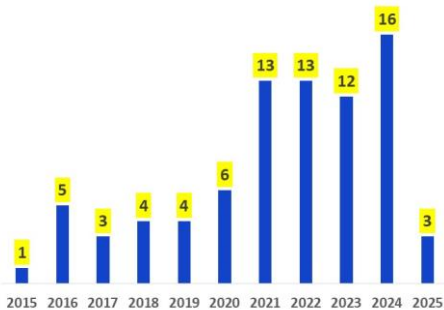
Şəkil 1. Scopus bazasında nəşrlərin tipə görə paylanması

Analoji olaraq, WoS bazasında da bu sahədə indeksləşən elmi nəşrlərin analizi aparılmışdır. Burada “Cyber Sovereignty” açar sözü ilə axtarıb etdikdə 59 elmi əsərə rast gəlinir ki, onların da tipə görə paylanması Şəkil 2-də göstərilmişdir.



Şəkil 2. Web of Science bazasında nəşrlərin tipə görə paylanması

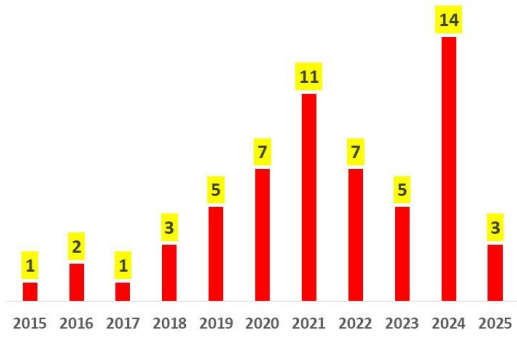
Bu elmi əsərlərin illər üzrə paylanması Şəkil 3-də göstərilmişdir. 80 elmi əsərin dillər üzrə paylanmasına baxdıqda isə 75-nin ingilis, digərlərinin isə çin, portuqal və rus dillərində olduğu məlum olur.



Şəkil 3. Scopus bazasında nəşrlərin illər üzrə paylanması

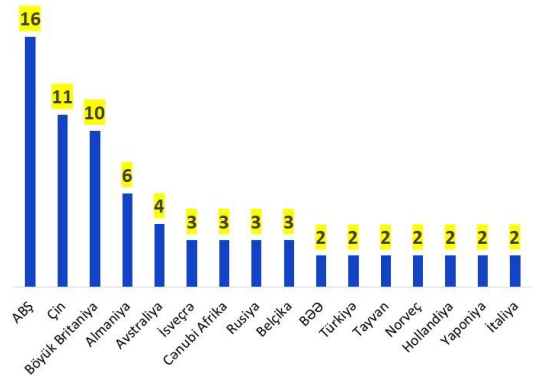
Şəkil 4-də Web of Science bazasında elmi əsərlərin illər üzrə paylanması göstərilmişdir. 59 elmi əsərin dillər üzrə

paylanmasına baxdıqda isə 55-i ingilis, digərlərinin isə ispan, fransız və norveç dillərində olduğunu qeyd etmək mümkündür.



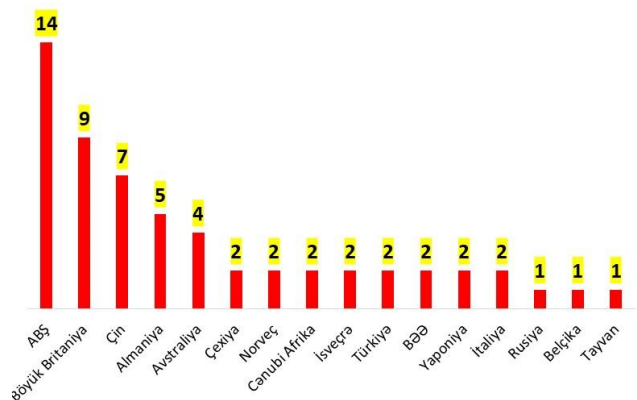
Şəkil 4. Web of Science bazasında nəşrlərin illər üzrə paylanması

Daha sonra Scopus bazasında indeksləşən məqalələrin coğrafiyasına baxdıqda (Şəkil 5) 32 ölkə arasında ABŞ, Çin və Böyük Britaniyanın üstünlük təşkil etdiyini vurğulamaq mümkündür.



Şəkil 5. Scopus bazasında nəşrlərin ölkələr üzrə paylanması

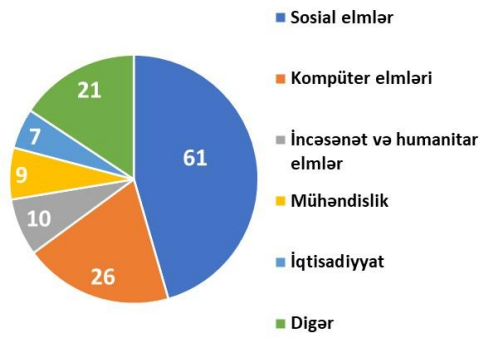
Şəkil 6-da WoS bazasında indeksləşən məqalələrin coğrafiyasına baxdıqda 28 ölkə arasında ABŞ, İngiltərə və Çin üstünlük təşkil etdiyini vurğulamaq mümkündür.



Şəkil 6. Web of Science bazasında nəşrlərin ölkələr üzrə paylanması

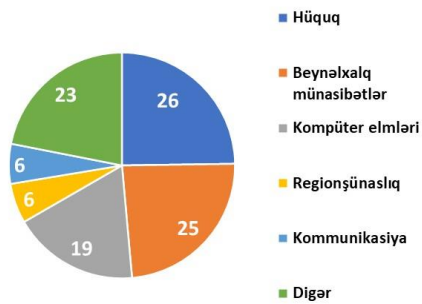
Şəkil 7-də Scopus bazasında bu istiqamətdə nəşr olunan elmi əsərlərin sahələr üzrə paylanmasına baxdıqda isə, sosial

elmlər (61 elmi əsər) və kompüter elmləri (26 elmi əsər) üstünlük təşkil edir.



Şəkil 7. Scopus bazasında nəşrlərin elm sahələri üzrə paylanması

Şəkil 8-də WoS bazasında bu istiqamətdə nəşr olunan elmi əsərlərin sahələr üzrə paylanmasına baxdıqda isə, hüquq (26 elmi əsər), beynəlxalq münasibətlər (25 elmi əsər) və kompüter elmləri (19 elmi əsər) üstünlük təşkil edir.



Şəkil 8. Web of Science bazasında nəşrlərin elm sahələri üzrə paylanması

Kompüter elmləri sahəsində kibersuverenlik ilə bağlı aparılan tədqiqatlarda kibersuverenlik və qlobal kiberməkanın idarə olunması, bu kontekstdə dövlətlərin suverenliyi beynəlxalq normativ çərçivələrlə necə tənzimlənməsi, kibertəhlükəsizliyə yenidən baxış və onun dövlət suverenliyinə təsiri, bir sıra ölkələrin (Türkiyə, Rusiya, Çin və s.) kibersuverenlik strategiyalarının təhlili, kiberməkanda neytrallığın öyrənilməsi və müxtəlif coğrafi regionlarda kiberməkanın təhlili, kibertəhlükəsizlik əməkdaşlığının vebometrik şəbəkə təhlili, milli kibertəhlükəsizlik strategiyalarının kibersuverenliyin inkişafına təsiri və s. kimi məsələlər araşdırılır.

III. KIBERSUVERENLİK İSTİQAMƏTİNDƏ TRENDLƏR

Tədqiqatlar və mövcud ədəbiyyatın analizi göstərir ki, hazırda dövlətlərin kibersiyasətini formalaşdıran beş əsas global trend mövcuddur:

Suveren infrastruktur və məlumatların lokaşdırılması: Dövlətlər vətəndaşlarına və kritik sistemlərə aid məlumatların ölkə hüdudlarından kənara çıxmasının qarşısını almaq üçün məlumat mərkəzlərinin milliləşdirilməsi

və xarici texnologiyalardan asılılığın azaldılması siyasətini yürüdür.

Süni intellekt, kvant texnologiyaları və suverenlik: Gələcəyin texnologiyaları hesab edilən süni intellekt alqoritmləri və kvant hesablamaları şifrələmə standartlarını dəyişdirmə potensialına malikdir. Dövlətlər bu texnologiyalara sahib olmaqla kiber üstünlüyü ələ almağa və suverenliklərini yeni dövrün çağırışlarına hazırlamağa çalışırlar.

Geosiyasi parçalanma və milli rəqəmsal suverenlik: Dünyada artan qütbləşmə qlobal internetin segmentasiyasına səbəb olur. Dövlətlər öz milli şəbəkələrini beynəlxalq internetdən təcrid edə biləcək rəqəmsal səddlər (məsələn, milli firewall sistemləri) yaradırlar.

Beynəlxalq hüquq və kiberməkanın tənzimlənməsi: Kiberməkanda tətbiq edilə biləcək beynəlxalq qanunların və davranış normalarının (BMT səviyyəsində) müzakirəsi və qəbulu istiqamətində diplomatik səylər gücləndirilir.

Kibersuverenlik və milli kiberdavamlılıq: Dövlətlər yalnız kiberməkanın qarşısını almağı deyil, həm də insident baş verdikdən sonra kritik sistemlərin fəaliyyətinin bərpası qabiliyyətini, yəni kiberdavamlılığı suverenliyin təməli şərti kimi qəbul edirlər.

NƏTİCƏ

Rəqəmsallaşmanın geniş vüsət aldığı müasir dövrdə kibertəhlükəsizlik və kibersuverenlik məsələləri milli təhlükəsizlik strategiyalarının ayrılmaz komponentlərinə çevrilmişdir. İKT-nin ictimai həyatın bütün sahələrinə nüfuz etməsi, dövlət və cəmiyyətlərin informasiya sistemlərindən asılılığını artırmaqla yanaşı, onları yeni tipli kibertəhdidlərə qarşı daha həssas vəziyyətə salır.

Scopus və Web of Science kimi beynəlxalq elmi bazalarda aparılan təhlillər bu sahədə artan elmi marağı və multidissiplinar yanaşmanı təsdiqləyir. Hər iki bazada “Cyber Sovereignty” üzrə elmi əsərlərin sayı illər keçdikcə artmaqda davam edir və əsasən sosial elmlər, hüquq, beynəlxalq münasibətlər və kompüter elmləri sahələrində cəmlənmişdir.

ƏDƏBİYYAT

- [1] L. Bornmann and R. Mutz, “Growth rates of modern science: A bibliometric analysis based on the number of publications and cited references,” *Journal of the Association for Information Science and Technology*, vol. 66, no. 11, pp. 2215–2222, 2015.
- [2] UNESCO, *Science, Technology and Innovation: Global Trends*. Paris, France: UNESCO Publishing, 2023. [Online]. Available: <https://uis.unesco.org/en/topic/science-technology-and-innovation>
- [3] Scopus, Available: <https://www.scopus.com>
- [4] Clarivate, Available: <https://clarivate.com>
- [5] G. J. Moore, “Huawei, cyber-sovereignty and liberal norms: China’s challenge to the West/Democracies,” *Journal of Chinese Political Science*, vol. 28, no. 1, pp. 151–167, 2023.
- [6] Y. Hong and G. T. Goodnight, “How to think about cyber sovereignty: The case of China,” *Chinese Journal of Communication*, vol. 13, no. 1, pp. 8–26, 2020.
- [7] M. C. Bartolomé, “Social media, disinformation, cyber sovereignty and digital surveillance,” *Revista de Estudios en Seguridad Internacional*, vol. 7, no. 2, pp. 167–185, 2020.

- [8] R. D. Taylor, “‘Data localization’: The Internet in the balance,” *Telecommunications Policy*, vol. 44, no. 8, 2020.
- [9] E. Matania and U. Sommer, “Tech titans, cyber commons and the war in Ukraine,” *International Relations*, 2023.
- [10] A. X. Wu and L. Z. Li, “Localism in Internet governance: The rise of China’s provincial web,” *China Information*, vol. 36, no. 2, pp. 262–282, 2022.
- [11] S. AlDaajeh, H. Saleous, and K. K. R. Choo, “The role of national cybersecurity strategies on the improvement of cybersecurity education,” *Computers & Security*, vol. 119, 2022.
- [12] M. L. Mueller, “Against sovereignty in cyberspace,” *International Studies Review*, vol. 22, no. 4, pp. 779–801, 2020.
- [13] A. Kokas, “The corporate cultivation of digital resignation in policymaking,” *Big Data & Society*, vol. 11, no. 4, 2024.
- [14] H. Shen, “China and global internet governance: Toward an alternative analytical framework,” *Chinese Journal of Communication*, vol. 9, no. 3, pp. 304–324, 2016.

Scientific Research in the Field of Cyber Sovereignty of the State: Multidisciplinary Analysis, Trends and Perspectives

Narmin Adigozalova

Institute of Information Technology, Baku, Azerbaijan

Abstract— Recently, the importance of cybersecurity and cyber sovereignty in the context of national security has been increasing. The main reason for this increase is the increased use of the digital environment by states, critical infrastructure and citizens. In the research work, the studies conducted in the direction of “Cyber Sovereignty” in the scientific databases Scopus and Web of Science were analyzed and the bibliometric analysis of the published works was conducted. The bibliometric analysis was conducted based on indicators such as years, languages, scientific fields and geographical distribution of the works published in this field. In addition, the results of the studies conducted in this direction during 2015-2025 were analyzed and the existing problems were identified.

Keywords— cyber sovereignty; bibliometric analysis; analysis of scientific works; international scientific database.