UOT 327
https://doi.org/10.59849/2710-0820.2025.1.187

Murad Rüstəmov
Naxçıvan Dövlət Üniversiteti, Müəllim
Azərbaycan
murad_rustemov@yahoo.com

MÜASİR DÜNYA SİYASƏTİNİN YENİ TENDENSİYASI: KİBERMƏKAN VƏ SİYASƏT

Açar sözlər*: *Kibertəhlükəsizlik, informasiya təhlükəsizliyi, milli təhlükəsizlik, dünya siyasəti, Amerika Birləşmiş Ştatları, BMT, kiber məkan.

Giriş

21-əsri İKT-siz təsəvvür etmək mümkünsuzdür və eləcədə bu sahənin əsas aspekti olan rəqəmsal medianın bizim həyat tərzimizə, ictimai-siyasi vərdişlərimizə çox böyük təsiri vardır. Bu gün biz müharibənin daha uzun, daha gizli, miqyasına, hədəflərinə və tempinə görə daha təəccüblü və başlanğıcı, sonu, rəqibləri və motivlərini ayırd etməyin daha çətin olduğu "Kiber Münaqişə" əsrinin astanasındayıq. Rəqəmsal media mühiti dinamikdir və demokratik idarəetmə və siyasət üçün ciddi nəticələri olan yeni, bəzən gözlənilməyən yollarla inkişaf etməyə davam edir. Bu media dövlət qurumlarının fəaliyyət tərzini, siyasi liderlərin ünsiyyət tərzini, seçkilərin mübahisələndirmə qaydasını və vətəndaş əlaqələrini kökündən dəyişdirib.Kibersiyasət bütün dünyada geniş istifadə olunan termindir və o, sosial proqram təminatının bütün formalarını əhatə edir. Bu və ya digər formada kiberməkan dediyimiz anlayış, hətta siyasi proseslərdə və bir sıra münaqişələrdə

Kiberməkan və dünya siyasəti

Müasir dövrdə dünyada siyasət sırf siyasi deyil, artıq texniki məsələlərə də istinad edə bilər. Son illərdə kibertəhlükəsizlik, internet azadlığı və idarəetmə də daxil olmaqla kiberməkan məsələləri sürətlə "siyasiləşdirilmiş" və təbii qlobal ictimai problemə çevrilmişdir.

Kiberdünyanın siyasiləşməsinin ən mühüm əlamətləri kimi kibertəhlükəsizliyin artıq ictimai-siyasi gündəmə daxil edilməsi, o cümlədən dünyada internet azadlığı siyasətinin yayılması və İT ictimai domen nəzəriyyəsinin təbliği və s. məsələləri göstərmək olar

Kiberməkan anlayışının dünyanı sürətlə siyasiləşdirə bilməsinin səbəbi İnternet təhlükəsizliyi üçün daxili aktuallıq və ABŞ-ın hegemonluğu saxlamaq üçün fəal təşviqi ilə bağlı siyasətçilərin və medianın yaratdığı təhdidlərlə sıx bağlıdır. Texniki məsələləri siyasiləşdirmək çox çətin olsa da, ölkələr təmasları artırmaq, konsensus yaratmaq, oxşar problemlərin həllində təcrübələri müqayisə etmək və öyrənmək və həddən artıq media təhdidlərini cilovlamaqla kiberməkanın siyasiləşdirilməsinin mənfi təsirini əhəmiyyətli dərəcədə azalda bilər.

Son illər beynəlxalq ictimaiyyət üç əsas qlobal ictimai problemin: maliyyə böhranı, iqlim dəyişikliyi və kiberməkan probleminin ortaya çıxmasının şahidi olub. Bunların arasında kiberməkan məsələsi xüsusilə diqqəti cəlb edir, çünki bu, beynəlxalq siyasi gündəmə sürətlə daxil olan yeni problemdir. Maliyyə böhranı və iqlim dəyişikliyi problemləri ilə müqayisədə kibertəhlükəsizlik problemi hələ də yeni inkişaf mərhələsindədir. Bunu tez-tez beynəlxalq istiqamətin və konsensus üçün hələ qlobal əsas və möhkəm qurulmuş beynəlxalq məsləhətləşmə sistemi formalaşmamış qanunların olmamasına görə "Wild West" ("Vəhşi Qərblə") ilə müqayisə etmək olar.

Kiberməkan elektron texnologiyanın tətbiqi ilə xarakterizə olunur. O, bir-biri ilə əlaqəli şəbəkə sistemləri və fiziki qurğular vasitəsilə məlumatları saxlayır, dəyişdirir və mübadilə edir. Bu, kompüterlər tərəfindən idarə olunan, əldə edilən və yaradılan çoxölçülü süni virtual dünyadır və mövcud dünyaya bağlıdır, bizim burada olduğumuz çox evrenli bir sistem yara-

dır, həm də virtual hər yerdə olma imkanı hansı ki biz ilə ora gedə bilərik.

Kiberməkanı iki növə bölmək olar: texniki məsələlər və qeyri-texniki məsələlər. Qeyri-texniki məsələlər beynəlxalq siyasət alimlərinin əsas tədqiqat mövzularıdır. Onlar əsasən üç əsas məsələdən ibarətdir: şəbəkə təhlükəsizliyi, İnternet azadlığı və yuxarıda qeyd edildiyi kimi onun idarə olunması.

Kibertəhlükəsizlik baxımından alimlər kibertəhlükəsizlik paradoksu ilə bağlı kiberməkanda bir sıra müzakirələr aparırlar. Köhnə deyimə görə, təhlükəsizlik ola bilməyəcəyi qədər paradoks: 'hər bir qanunda bir boşluq var': Digər təhlükəsizlik problemləri kiber müharibə və kiber çəkindirmədir.

İnternet azadlığı Amerika Birləşmiş Ştatların son illərdə güclü şəkildə irəli sürdüyü xarici siyasət silahıdır və İnternetin ictimai sahəsi nəzəriyyəsi beynəlxalq münasibətlərin bu konsepsiyasını gücləndirmək üçün mühüm nəzəri əsasdır. Bu sahədə aparılan tədqiqatlar kiberməkanın qlobal ictimai mülkiyyətinə və internet azadlığı ilə kibertəhlükəsizlik arasındakı ziddiyyətə diqqət yetirir.

Kibertəhlükəsizlik problemləri artdıqca və ABŞ-ın internet azadlığı siyasəti həyata keçirildikcə kiberməkanın riskləri tədricən ölkələr arasında qarşılıqlı etimad və normal mübadilə üçün ciddi maneəyə çevrilir. Bu səbəbdən, şəbəkə təhlükəsizliyi tədbirləri və kibercinayətkarlıq problemlərinə cavab da daxil olmaqla İnternet idarəçiliyi beynəlxalq siyasət alimlərinin də maraqlandığı mühüm məsələyə çevrilmişdir.

Kiberməkan problemi yeni yaranmaqda olan qlobal ictimai problemdir. Bu kimi mövzular üzrə tədqiqatlar, xüsusilə nəzəri təhlillər hələ də sürətli inkişaf mərhələsindədir, lakin inkişaf sürəti demək olar ki qənaətbaxış hesab etmək olar. Şəbəkə təhlükəsizliyini nümunə götürsək, insanlar şəbəkə təhlükəsizliyi anlayışının konnotasiyasını müxtəlif şərh edirlər və çox vaxt onu kompüter təhlükəsizliyi, şəbəkə təhlükəsizliyi və informasiya təhlükəsizliyi kimi terminlərlə əvəz edir.

Kibertəhlükəsizliyin müxtəlif problemləri rəsmi sənədlərdə, mediada və İT-də geniş şəkildə qeyd olunsa da, təəccüblüdür ki az sayda təhlükəsizlik üzrə tədqiqat işi təhlükəsizlik və İT-nin birləşməsini aydın şəkildə izah edir. İohan Erikssonun 2006-cı ildəki informasiya inqilabının təhlükəsizliyə təsiri ilə bağlı təhlilinin təqdim etdiyi xülasədən bugünkü kompüter təhlükəsizliyi araşdırmalarını qiymətləndirmək hələ də çox məqsədəuyğundur: "Tədqiqatların əksəriyyəti etibarsızdır və diqqət informasiya texnologiyaları ilə bağlı təhlükəsizlik məsələlərinə yönəlib. İT ədəbiyyatının əksəriyyəti siyasət yönümlüdür və nadir hallarda beynəlxalq münasibətlər nəzəriyyəsi və ya hər hansı digər fənlərlə əlaqəlidir. Üstəlik və bəlkə də daha önəmlisi, çox az sayda alimi kiberməkan məsələsinin dünyada sürətlə siyasiləşə bilməsinin səbəbi maraqlandırır. Başqa sözlə desək, kiberməkan əvvəlcə texniki, ardınca daxili siyasi, nəhayət, beynəlxalq siyasi məsələdir.

Qlobal ictimai problemlər müxtəlifdir, lakin onların heç də hamısı açıq-aydın beynəlxalq siyasi məsələlərə çevrilə bilməz. Siyasiləşmə sözünün iki mənası var: biri siyasi mahiyyətin verilməsi prosesi, digəri isə siyasi mahiyyət əldə etməyin nəticəsidir. Daxili siyasətdə siyasiləşməyə çox vaxt fərdi siyasi şüurun formalaşması və iştirakının davamı kimi baxılır.

Kiberməkan məlumatı saxlamaq və istifadə etmək və ünsiyyət qurmaq qabiliyyətinə malik bir-biri ilə əlaqəli kompüter cihazlarından ibarətdir. O, dörd təbəqədən ibarətdir: insanlar, məlumat, məntiqi modullar və fiziki qurğular. İstifadə və ya məqsəd baxımından kiberməkan məlumat və məlumatı manipulyasiya etmək, emal etmək və inkişaf etdirmək üçün istifadə oluna bilər və insanlar arasında ünsiyyəti və insanlar və informasiya arasında qarşılıqlı əlaqəni inkişaf etdirə. Bir tərəfdən, dörd təbii fəzadan – yerüstü, dəniz, atmosfer və "ayaltı" məkandan fərqli olaraq, kiberməkan tamamilə insan tərəfindən yaradılmış məkandır, rəqəmsal və virtual isə onun mühüm xüsusiyyətləridir. Digər tərəfdən, dörd təbii məkandan fərqli olaraq, kiberməkan getdikcə daha çox neo-siyasət əlamətləri göstərir.

Konkret olaraq, kiberməkanın qlobal siyasiləşməsi sürətlə gündəlik həyatın bir hissəsinə çevrilən kibertəhlükəsizlikdə özünü göstərir. Məsələnin siyasiləşdirilməsinin fundamental təzahürü ondan ibarətdir ki, bu, beynəlxalq danışıqların məzmununa çevrilib və müvafiq beynəlxalq təşkilatlar tədricən problemlə maraqlanmağa başlayıblar.

Yeni əsrdən etibarən kibertəhlükəsizlik məsələsi Birləşmiş Millətlər Təşkilatının mühüm mövzusuna çevrilib. Birləşmiş Millətlər Təşkilatı beynəlxalq ictimaiyyətin diqqətini kibertəhlükəsizlik təhdidlərinə və əməkdaşlığa cəlb etmək üçün bir sıra qətnamələr qəbul etmişdir.

Baş Assambleyanın 22 yanvar 2001-ci il tarixli 55/63 saylı Qətnaməsi təklif edir ki, ölkələr öz qanunlarının və təcrübələrinin informasiya texnologiyalarından qeyri-qanuni istifadə edən şəxslər üçün təhlükəsiz sığınacaqları aradan qaldıra bilməsini təmin etməlidir. Araşdırma aparılarkən informasiya texnologiyalarından qeyri-qanuni sui-istifadə ilə bağlı beynəlxalq hallar cinayət məsuliyyətinə cəlb edilməlidir. Buna görə də aidiyyəti dövlətlər hüquq-mühafizə orqanlarının koordinasiyası ilə əməkdaşlıq etməlidirlər. İnformasiya texnologiyalarından qeyri-qanuni sui-istifadə ilə mübarizədə ölkələr ən ciddi problemlər haqqında məlumat mübadiləsi aparmalıdırlar. Baş Assambleyanın 6 yanvar 2006-cı il tarixli 60/45 saylı qətnaməsi BMT Baş Katibindən potensial informasiya təhlükəsizliyi təhdidləri ilə bağlı mümkün əməkdaşlığa dair araşdırmaları davam etdirmək üçün hökumətlərarası ekspert qrupu təyin etməyi tələb edir və qrupdan hesabat təqdim etməyi tələb edir. Bu qətnamə və tövsiyələr informasiya təhlükəsizliyi üzrə beynəlxalq konvensiyanın standartlarından uzaq olsa da, informasiya təhlükəsizliyi məsələlərinin – ortaya çıxan problem kimi – bütün dünyada diqqəti cəlb etməsi deməkdir.

Nəticə. Məqalədə siyasi proseslərdə qarşıdurma zamanı kiber münaqişələrin nəzəri və praktiki forması informasiya təhlükəsizliyinə və təhlükəsizlik sisteminə təsirinə milli və beynəlxalq yanaşmaların kombinasiyası ilə təhlil edilir.

Kiberməkanın mühafizəsi ərazi sərhədləri ilə məhdudlaşmır, ona görə də kiberməkan sahəsində beynəlxalq tərəfdaşlıq rəqibə siyasi təsir nəticəsində kibercinayətlərin tədqiqi sahəsində dövlətlərarası tərəfdaşlıq səviyyəsində əməkdaşlığın müasir mütərəqqi qoludur. Beləliklə kibermüdafiə proseslərində fərdi mübarizə qlobal dünyada o qədər də effektiv deyil.

Ədəbiyyat

1. Anderson, R., Barton, C., Boehme, R., Clay ton, R., van Eeten, M. J. G., Levi, M., Moore, T. & Savage, S. Measuring the cost of cybercrime. URL: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf 2012 115 p.
2. Arquilla, J. *Ethics and Information Warfare. In Strategic Appraisal: The Changing Role of Information in Warfare.* Ed. by Z. Khalilzad, J. White & A. Marsall. Santa Monica: RAND Corporation. 2019, 255 p.
3. Bell, D. The Social Framework of the Infor
4. Buzan, B., Wæver O. & et al. *Security: A new framework for Analysis.* Boulder: Lynne Rienner Publishers. 1998, 28 p.
5. Chin V.A., & Shahalami, I. Y. Analysis and synthesis of the requirements for safety systems of objects of critical information infrastructure. *Issues of cybersecurity*. 2013, 125 p.
6. For a discussion of the military revolution that emerged between the two world wars. In: *Military Innovation in the Interwar Period*. Ed. by W. Murray & A. R. Millett. Cambridge: Cambridge University Press. 2016, pp. 299-302.
7. Freedman, L. International Security: Changing Targets. *Foreign Policy*, 1998, 48-63 s.
8. Matveev, B. Status and prospects of development of national information security industry in 2014. *Cybersecurity*, 2013, pp. 61-64.
9. Metz, S., & Kievit, J. *Strategy and the Revolution in Military Affairs: From Theory to the Police.* Strategic Studies Institute. 2010, pp. 33-34.
10. Rosenzweig, P. The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence. *Deterring Cyberattacks: Informing Strategies and Developing Options*. National Research Council, 2010, 269 p.

Summary

Murad Rustamov

World politics and cyberspace

Cybersecurity, with its significant role in world politics, is applied across various domains related to national security. This issue spans from diplomatic relations to the strategic planning of international organizations.

This article delves into the importance of cybersecurity in global politics. In the 21st century, one of the national security, public safety, and economic challenges faced by every country is the threat of cybersecurity vulnerabilities. Cybersecurity has become an inherent feature of modern life, connecting the global population through cyberspace for social interaction and organizational purposes. Cyberspace is a defining characteristic of contemporary life, where individuals and communities engage and organize.

The existence of numerous cybersecurity issues across different sectors naturally increases their political significance. From specific cases to national and international levels, the need for cybersecurity grows - it becomes a central concern in diplomacy and world politics.

The research in this article aims to demonstrate how cybersecurity serves as a tool for political interests and its place in global politics. It emphasizes the importance of focusing on information security and national security in the context of cybersecurity.

The article discusses methods used by national security institutions and international organizations to address cybersecurity threats, covering both theoretical and practical aspects. Cybersecurity's broad application extends from diplomatic relations to the strategic planning of international organizations.

Keywords: *Cyber security, information security, national security, world politics, United States of America, UN, cyberspace*

Резюме

Мурад Рустамов

Мировая политика и киберпространство

Кибербезопасность стала одним из основных инструментов в руках государств и в руках формально союзных организаций. Она включает в себя дипломатические взаимодействия и тактики международных сущностей. Эта проблема охватывает дипломатические отношения и стратегии международных организаций.

В этой статье я проанализирую роль кибербезопасности в контексте международных отношений. В 21 веке для любого государства одной из угроз национальной безопасности, общественной безопасности и экономики являются киберугрозы. Кибербезопасность возникла как один из основных аспектов жизни, одновременно объединяя людей по всему миру с целью социальной интеракции и координации через виртуальный мир.

Существование множества вызовов в области кибербезопасности в различных секторах, естественно, способствует увеличению их значимости для политики. От отдельных случаев до национального и глобального уровней, спрос на кибербезопасность постоянно растет – это становится основной областью дипломатии и международных отношений.

Цель исследования в этой статье – предоставить доказательства того, как кибербезопасность используется как средство для достижения определенных политических целей, и какую роль она играет в более широком контексте международных отношений. Вопросы ин-

формации и национальной безопасности с отсылкой к кибербезопасности нуждаются в особом внимании.

Статья сосредоточена на методах, используемых национальными учреждениями безопасности и международными организациями для решения угроз кибербезопасности, учитывая как теоретические, так и практические аспекты. Кибербезопасность применяется во многих сферах, включая дипломатические отношения и стратегическое планирование международных организаций.

Ключевые слова: *кибербезопасность, информационная безопасность, национальная безопасность, мировая политика, США, ООН, киберпространство*