UOT: 327, 327.5, 32, 320

AYNUR ƏLİŞANOVA
Azərbaycan Respublikası Prezidenti Yanında Dövlət İdarəçilik Akademiyası
Dövlət Qulluğu və Kadr Siyasəti kafedrasının müəllimi
a.aynour@hotmail.com

BEYNƏXLAQ HÜQUQ VƏ RƏQƏMSAL ANARXİYA: BEYNƏLXALQ TƏŞKİLATLAR YENİ KİBER VƏ VİRTUAL KONFRLİKTLƏRƏ NECƏ UYĞUNLAŞIR

DOI: https://doi.org/10.36719/2708-065X/112/61-65

Məqalənin məqsədi beynəlxalq hüququn yeni təhlükəsizlik mühitinə uyğunlaşmaqda qarşılaşdığı çətinlikləri araşdırmaqdır. Xüsusilə, məqalədə mövcud hüquqi sistemin yetərsiz qaldığı üç sahə təhlil edilir. İlk olaraq, Meta-məkanın yeni münaqişə sahəsi kimi meydana çıxması və virtual mühitləri, mərkəzləşdirilməmiş platformaları və rəqəmsal identiklikləri tənzimləyən yurisdiksiya normalarının olmaması. İkinci olaraq, rəqəmsal suverenlik və AI əsaslı hərbiləşmə, o cümlədən süni intellekt silahlarının yaratdığı problemlər və mövcud humanitar hüququn avtonom sistemləri tənzimləməkdə aciz qalması. Daha sonra isə beynəlxalq təşkilatların institusional reaksiyaları və artan kibertəhdidlərə cavabları, bu reaksiyaların məcburi qlobal normalar yaratmaqda məhdud imkanları. Bu təhlillərə əsaslanaraq məqalə əsas bir suala cavab axtarır: Kiberkonflikt və AI ilə gücləndirilmiş müharibə üçün xüsusi hazırlanmış yeni bir Cenevrə Konvensiyasına ehtiyac varmı?

Məqalədəki bölmələr kibər əməliyyatların yaratdığı konseptual və hüquqi çətinlikləri araşdırır, mövcud beynəlxalq tənzimləyici çərçivənin qeyri-birləşmiş və fragmentar xarakterini qiymətləndirir və hərtərəfli saziş modeli üçün mövcud təklifləri təhlil edir. Hüquqi təhlilləri müasir kibertəhlükəsizlik sahəsindəki elmi araşdırmalarla birləşdirərək, məqalə iddia edir ki, mövcud beynəlxalq sistem rəqəmsal münaqişəni idarə etmək üçün kifayət qədər təchiz olunmayıb. Nəticə olaraq vurğulanır ki, Cenevrə Konvensiyasının hazırlanması bir müddət qlobal sabitliyi qorumaq və rəqəmsal dövrdə mülki şəxslərin müdafiəsini təmin etmək baxımından zəruri ola bilər, lakin, bunun effektivliyi sual altındadır.

Açar sözlər: Kiber müharibə, Rəqəmsal anarxiya, Beynəlxalq hüquq, Meta-məkan, Rəqəmsal suverenlik, Virtual konfliktlər, Cenevrə Konvensiyaları.

Giriş. Sürətlə inkişaf edən kiberməkan süni intellekt (AI) və virtual mühitlər qlobal təhlükəsizliyi ənənəvi döyüş meydanından xeyli kənara daşıyıb və immersiv virtual mühitlərdə baş verən illəriləyişlərin təsiri ilə dərin bir transformasiya keçirmişdir. Bu gün siyasi, iqtisadi və hərbi gərginliklər təkcə quru, dəniz və hava üzərində deyil, həm də meta-məkanlarda, qlobal məlumat infrastrukturunda və alqoritmlərin idarə etdiyi ekosistemlərdə baş verir. Lakin bu dərin transformasiyaya baxmayaraq beynəlxalq hüquq rəqəmsal suverenlik, AI əsaslə silahlar və kiberkonfliklərlə bağlı aydın normalara malik deyil. Bu boşluq bir çox tədqiqatçıların "rəqəmsal anarxiya" adlandırdığı vəziyyəti yaradır və bu da dövlətlərin dəqiq hüquqi məhdudiyyətlər olmadan hərəkət etdiyi bir sahəni təşkil edir.

Kiberhücumlar daha mürəkkəb olduqca və virtual məkanlar getdikcə geosiyasi arenalara bənzədikcə, əsas bir sual ortaya çıxır: Kiberkonflikt üçün xüsusi hazırlanmış yeni bir Cenevrə Konvensiyasına ehtiyac varmı?

Sürətlə genişlənən kiberməkan, süni intellekt (AI) və immersiv virtual platformalar müasir təhlükəsizlik mühitini əsaslı şəkildə dəyişdirmişdir. Dövlətlər və qeyri-dövlət aktorları artıq strateji məqsədlərinə təkcə ənənəvi hərbi vasitələrlə deyil, həm də kiber əməliyyatlar, alqoritmik manipulyasiya və virtual mühitlərdə həyata keçirilən fəaliyyət vasitəsilə nail olmağa çalışırlar. Bu sahələr milli gücün və geosiyasi rəqabətin mərkəzinə çevrildikcə, ənənəvi beynəlxalq hüququn zəifliklərı daha aydın görünür. Kinetik münaqişə, ərazi suverenliyi və insan tərəfindən idarə olunan silahlar üçün yaradılmış hüquqi rejimlər kiberhücumları, AI əsaslı silahlar və meta-məkan əməliyyatlarını tənzimləməkdə çətinlik çəkir [1]. Bu məqalə beynəlxalq hüququn bu texnoloji dəyişikliklərə necə reaksiya verdiyini araşdırır. Tədqiqat üç əsas istiqmətə fokuslanır: meta-məkanın yeni münaqişə sahəsi kimi formalaşması, rəqəm-

sal suverenlik və AI-nin hərbiləşməsinin yüksəlişi, həmçinin BMT (Birləşmiş Millətlər Təşkilatı) , NATO (Şimalı Atlantika Müqaviləsi Təşkilatı) və Aİ (Avropa İttifaqı) kimi beynəlxalq təşkilatların institusional uyğunlaşma səyləri. Müzakirə sonda artmaqda olan normativ boşluğu aradan qaldırmaq üçün kibermünaqişələrə dair yeni bir Cenevrə Konvensiyasına ehtiyacın olub-olmamasını qiymətləndirir.

Atributika çətinlikləri, mərkəzləşdirilməmiş infrastrukturlar və özəl aktorların prosesə cəlb olunması suverenlik və ərazi arasında olan klassik əlaqəni sarsıdır [2]. Bundan əlavə, ortaya çıxan AI əsaslı silah sistemləri fərqləndirmə, proporsionallıq və insan məsuliyyəti kimi əsas humanitar prinsiplərə yeni təhlükələr yaradır [3]. Tədqiqatlara əsasən, kibər əməliyyatlar getdikcə daha çox mülki rəqəmsal infrastrukturun, seçkilərin, xəstəxanaların, enerji şəbəkələrinin və virtual identikliklərin hədəfinə çevrildikcə, nəticələr miqyas və dağıdıcı təsir baxımından ənənəvi silahlı hücumlara bənzəməyə başlayır. 2021-ci ildə ABŞ-da Colonial Pipeline-a edilən ransomware hücumu ölkənin Şərq Sahilində ən böyük yanacaq boru kəmərinin fəaliyyətinin dayanmasına səbəb olmuş, nəticədə bir neçə ştatda genişmiqyaslı yanacaq qıtlığı yaranmışdır. Bu hadisə kibərhücumların fiziki sabotajla müqayisə oluna biləcək dərəcədə milli səviyyədə iqtisadi pozuntu yarada biləcəyini göstərən ən bariz nümunələrdən biridir.

Meta-məkanın yeni münaqişə sahəsi kimi formalaşması. Meta-məkan istifadəçilərin və dövlətlərin sosial, iqtisadi və siyasi fəaliyyətlərini getdikcə daha çox həyata keçirdiyi qarşılıqlı əlaqəli virtual mühitləri, artırılmış reallıq platformalarını, mərkəzləşdirilməmiş şəbəkələri və inkişaf etməkdə olan metaverse sistemlərini ifadə edir [6]. Tədqiqatlara əsasən, meta-məkan isə əsasən Web3 texnologiyaları üzərində qurulub. Halbuki, Web2 saytları mərkəzləşdirilmiş serverlərdən istifadə edir, metavers saytları isə yerləşdirmə üçün blokçeyn texnologiyasından istifadə edir ki, bu da onları mərkəzləşdirilməmiş edir. Səbəb odur ki, bütün Web3 konsepti mərkəzləşdirilməməyə və internetin senzurasız versiyasını yaratmağa əsaslanır [7]. Buna görə də bu əsaslı mühitlər kimi platformalar dövlət hakimiyyəti əvəzinə öz qaydaları ilə fəaliyyət göstərir. Nəzərə alsaq ki, istifadəçilər və serverlər müxtəlif ölkələrdə yerləşir, bu da hansı dövlətin qanunlarına görə tətbiq olunacağını müəyyənləşdirməyi çətinləşdirir. Hüquqi məsuliyyət də aydın deyil, çünki platformalar DAO-lar, anonim yaradıcılar və smart-müqavilələr vasitəsilə idarə olunur. Bu səbəbdən kiberhücumlar, virtual əmlak oğurluqları və NFT fırıldaqları kimi cinayətlərin araşdırılması çətinləşir. Eyni zamanda, bir fəaliyyət bir neçə ölkənin qanunlarını poza bilər və dövlətlərin səlahiyyətləri toqquşa bilər. Nəticədə, bu göstəricilər boz sahəyə düşür və ənənəvi dövlət səlahiyyəti mərkəzləşdirilməmiş meta-məkanlarda birbaşa tətbiq oluna bilmir, bu isə beynəlxalq hüquqda suverenlik, məsuliyyət və cinayətlərin təsnifi məsələlərini qeyri-müəyyən edir. Bu mühitlərdə suverenliyin pozulması və ya silahlı hücumun nədən ibarət olduğuna dair dəqiq bir tərif yoxdur ki, bu da BMT Nizamnaməsinin və beynəlxalq adət hüququnun tətbiqini çətinləşdirir [8]. Meta-məkanda aydın qaydaların olmaması "rəqəmsal anarxiya"ya səbəb olub [9]. Dövlətlər və qeyri-dövlət aktorları hüquqi qeyri-müəyyənlikdən istifadə edərək minimum nəticələrlə fəaliyyət göstərirlər. 2014-cü ildə Şimali Koreyanın *Sony Pictures*-a etdiyi kiberhücum, məlumatların oğurlanması, əvvəlcə bir Amerika şirkəti üçün ictimai utanca səbəb oldu, bu problem, çətinlik e-poçtların sızdırılması və əməliyyatların pozulması ilə nümayiş etdirilmişdir [10]. Mərkəzləşdirilməmiş virtual mühitlərdə cinayətkarın müəyyən edilməsi daha da çətinləşir ki, bu da məsuliyyətin müəyyənləşdirilməsini mürəkkəbləşdirir. Hadisə həmçinin kiber sahədə hücumlara cavab vermək üçün çoxsahəli qarşısının alınması (multi-domain deterrence) rolunu aydınlaşdırır [10].

Rəqəmsal suverenlik - dövlətlərin sərhədləri daxilində məlumatlara, infrastruktur və süni intellekt (AI) sistemlərinə nəzarət qabiliyyəti, mərkəzi təhlükəsizlik məsələsinə çevrilib və ölkələr fərqli yanaşmalar tətbiq edirlər. Avropa İttifaqı GDPR, NIS2 və AI Aktı vasitəsilə məlumatları, kritik infrastrukturu və AI-nı tənzimləyir [12]. Çin isə Kiber Təhlükəsizlik və Məlumat Təhlükəsizliyi Qanunları ilə rəqəmsal platformalara və yerli məlumatlara ciddi nəzarət tətbiq edir [15]. Halbuki, ABŞ strateji azadlığa üstünlük verir, proaktiv kiber əməliyyatlar həyata keçirir və beynəlxalq məhdudiyyətlərə qarşı çıxır [13]. Avtonom AI silahları Beynəlxalq Humanitar Hüquq (IHL) prinsipləri olan fərqləndirmə, proporsionallıq və məsuliyyətə [16] meydan oxuyur, nəticədə məsuliyyət boşluqları, proqnozlaşdırılmazlıq və proporsionallıq uğursuzluqları yaranır.

Buna baxmayaraq ki, Beynəlxalq Məhkəmə 1996-cı ildə təsdiqlədi ki, Beynəlxalq Humanitar Hüquq (IHL) bütün silahlara, "gələcəkdəki silahlar da daxil olmaqla," tətbiq olunur və bu, silahlı qarşı-

durma zamanı kiber əməliyyatları da əhatə edir, Beynəlxalq Qırmızı Xaç Komitəsi (ICRC) bu fikri dəstəkləyir və bildirir ki, silahlı qarşıdurma zamanı kiber əməliyyatlar kinetik hərəkətlər kimi IHL-ə uyğundur. Lakin, Microsoft-un Prezidenti – Brad Smitub irəli sürdüyü Kiber Cenevrə Konvensiyası sual altındadır.

Bəzi alimlər iddia edirlər ki, Kiber Cenevrə Konvensiyası meta-məkandakı mülki şəxsləri qorumaq, AI silahlarını tənzimləmək, dövlət məsuliyyətini müəyyənləşdirmək və rəqəmsal suverenliyi aydınlaşdırmaq üçün normaları kodlaşdıra bilər. Belə bir müqavilə eskalasiyanın qarşısını ala, hüquqi aydınlıq təmin edə və getdikcə daha çox mübahisəli olan rəqəmsal və meta-məkan sahələrində mülki rəqəmsal aktivlərin qorunmasını təmin edə bilər.

Bəzi alimlər isə buna qarşı çıxır, əsasən aşağıdakı səbəblərə görə:

Müəyyənlik çatışmazlığı: Hücum edənlərin kimliyi aydın olmadıqda məsuliyyətin təyin olunması çətindir.

Siyasi parçalanma: Yüksələn millətçilik, çox tərəfli əməkdaşlığın zəifləməsi və texno-strateji rəqabətlər qlobal konsensusun əldə edilməsini çətinləşdirir.

Uyğunlaşma problemləri: Köhnə müqavilələr danışıqlar və yenilənmə baxımından ləngdir, halbuki kibertexnologiyalar sürətlə inkişaf edir [17].

Nəticə. Beləliklə, Kiber Cenevrə Konvensiyasının tətbiqi və təsdiqi bir sıra səbəblərə görə sual altındadır. Yuxarda Swarnali Goshun tədqiqatında göstərilən səbəblərdən, Konvensiyanın effektivliyi və tətbiq olunma perspektivi hələ tam aydın deyil və beynəlxalq ictimaiyyət arasında müzakirə mövzusudur. Hazırkı mənzərə isə hibrid yanaşmanı təklif edir: Beynəlxalq Humanitar Hüququn (BHH) tətbiqini ekspert analizi vasitəsilə aydınlaşdırmaq, məsələn, Tallinn Manual kimi təşəbbüsləri dəstəkləmək. Belə ekspert əsaslı çərçivələr qanuni davranışı istiqamətləndirə və hüquqi qeyri-müəyyənliyi azalda bilər.

ƏDƏBİYYAT

1.Ioan-Andrei Cursaru. (2024, January 19). Adapting to the Future: Navigating the Evolving Security Landscape. CYIS. https://www.cyis.org/post/adapting-to-the-future-navigating-the-evolving-security-landscape [03.12.2025].
2.Eichensehr, K.E. (2019). Decentralized Cyberattack Attribution. AJIL Unbound, 113 (doi:10.1017/aju.2019.33), 213-217. https://doi.org/10.1017/aju.2019.33
3.Pooja, & Singh, B. (2025). Autonomous Weapons And The Future Of Armed Conflict: A Threat To International Humanitarian Law? EPRA International Journal of Research and Development (IJRD), 10 (7). https://doi.org/10.36713/epra23006
4.Rushing, E. (2023, October 19). Protecting civilians against digital threats: four worrying trends and recommendations to address them. Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2023/10/19/protecting-civilians-digital-threats-four-worrying-trends/ [03.12.2025].
5.Easterly, J., & Fanning, T. (2023, May 7). The attack on colonial pipeline: What we've learned & what we've done over the past two years. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years [03.12.2025].
6.Ritterbusch, G. D., & Teichmann, M. R. (2023). Defining the Metaverse: A Systematic Literature Review. IEEE Access, 11(11), 12368–12377. https://doi.org/10.1109/access.2023.3241809
7.Namezage. (2025). What is a Metaspace - Explained | Namezage. Namezage.com. https://namezage.com/learning-hub/metaspace-explanation/ [03.12.2025].
8.Jordan, L. (2024). Unwilling or Unable. Stockton Center for International Law, 103(2024). https://digitalcommons.usnwc.edu/cgi/viewcontent.cgi?article=3071&context=ils [03.12.2025].
9. Zamfiroiu, A., Ciupercă, E. M., Voicu, S., Cîrnu, C.-E., & Vevera, A.-V. (2024). Reziliența comunității în Metavers prin adoptarea de strategii pentru detectarea dezinformării digitale. Revista Română de Informatică Și Automatică, 34(3), 23-34. https://doi.org/10.33436/v34i3y202402
10. Desimone, A., & Horton, N. (2017). The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace Nightmare.

11. National Security Report. - https://www.jhuapl.edu/sites/default/files/2022-12/SonyNightmareBeforeChristmas.pdf [03.12.2025].
12. Arand, D. (2025, December 2). From GDPR to AI Act: The Evolution of Data and AI Security in the EU. Cyera.com; Cyera. https://www.cyera.com/blog/from-gdpr-to-ai-act-the-evolution-of-data-and-ai-security-in-the-eu [03.12.2025].
13. Department of Defence, US. (2023). Summary 2023 Cyber Strategy of Department of Defence. - https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF [03.12.2025].
15. Lafollette, B. (2025, March 17). Security Over Growth: How China's Data Security Laws Are Driving Foreign Investment Away. Yale's Undergraduate Magazine on U.S.-China Relations. - https://chinahandsmagazine.org/2025/03/17/security-over-growth-how-chinas-data-security-laws-are-driving-foreign-investment-away/ [03.12.2025].
16. ICRC. (2003). Advisory Service International Humanitarian Law and International Human Rights Law Similarities and differences. - https://www.icrc.org/en/document/international-humanitarian-law-and-international-human-rights-law-similarities-and [03.12.2025].
17. Ghosh, S. (2025, November 7). The Geneva Conventions of Cyber Warfare: Do We Need a New Set of Rules? IronQlad. https://www.ironqlad.ai/post/the-geneva-conventions-of-cyber-warfare-do-we-need-a-new-set-of-rules [03.12.2025].

АЙНУР АЛИШАНОВА
Академия государственного управления при Президенте Азербайджанской Республики
Кафедра государственной службы и кадровой политики

МЕЖДУНАРОДНОЕ ПРАВО И ЦИФРОВАЯ АНАРХИЯ: КАК МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ АДАПТИРУЮТСЯ К НОВЫМ КИБЕР- И ВИРТУАЛЬНЫМ КОНФЛИКТАМ

Цель данной статьи - изучить проблемы, с которыми сталкивается международное право при адаптации к новой среде безопасности. В частности, анализируются три взаимосвязанные области, в которых существующая правовая система остаётся недостаточной. Во-первых, появление метапространства как новой области конфликта и отсутствие юрисдикционных норм, регулирующих виртуальные среды, децентрализованные платформы и цифровые идентичности. Во-вторых, цифровой суверенитет и милитаризация на базе ИИ, включая проблемы, создаваемые оружием с элементами искусственного интеллекта, и неспособность существующего гуманитарного права регулировать автономные системы. Наконец, институциональные ответы международных организаций и их реакции на рост киберугроз, а также ограниченные возможности таких ответов по созданию обязательных глобальных норм. Исходя из этого анализа, статья стремится ответить на ключевой вопрос: необходима ли новая Женевская конвенция для киберконфликтов и войн с использованием ИИ?

В последующих разделах рассматриваются концептуальные и правовые проблемы, возникающие при кибероперациях, оценивается фрагментарный и неунифицированный характер существующей международной нормативной базы, а также анализируются существующие предложения по созданию комплексной модели договора. Объединяя юридический анализ с современными исследованиями в области кибербезопасности, статья приходит к выводу, что существующая международная система недостаточно подготовлена для регулирования цифровых конфликтов. Соответственно, в заключении подчёркивается, что разработка Кибер-Женевской конвенции может быть необходима для защиты глобальной стабильности и обеспечения защиты гражданских лиц в цифровую эпоху.

Ключевые слова: Кибервойна, Цифровой анархизм, Международное право, Метапространство, Цифровой суверенитет, Виртуальные конфликты, Женевские конвенции.

AYNUR ALISHANOVA
Academy of Public Administratio under the President of the Republic of Azerbaijan
Department of Public Service and Personnel Policy

INTERNATIONAL LAW AND DIGITAL ANARCHY: HOW INTERNATIONAL ORGANIZATIONS ADAPT TO NEW CYBER AND VIRTUAL CONFLICTS

This article aims to examine the challenges international law faces in adjusting to the new security environment. In particular, it analyzes three interrelated areas in which the existing legal system remains insufficient. First, the emergence of meta-space as a new domain of conflict and the absence of jurisdictional norms regulating virtual environments, decentralized platforms, and digital identities. Second, digital sovereignty and AI-based militarization, including the challenges posed by artificial intelligence weapons and the inability of existing humanitarian law to regulate autonomous systems. Finally, the institutional responses of international organizations and their reactions to increasing cyber threats, as well as the limited capacity of such responses to create binding global norms. Based on these analyses, the article seeks to answer the core question: Is a newly formulated Geneva Convention for cyber conflict and AI-enhanced warfare necessary?

The following sections examine the conceptual and legal challenges generated by cyber operations, assess the fragmented and non-unified nature of the current international regulatory framework, and analyze existing proposals for a comprehensive treaty model. By combining legal analysis with contemporary research in the field of cybersecurity, the article argues that the existing international system is not sufficiently equipped to govern digital conflict. Accordingly, the conclusion emphasizes that developing a Cyber Geneva Convention may be necessary for protecting global stability and ensuring the protection of civilians in the digital age. However, its effectiveness remains uncertain.

Keywords: Cyber warfare, Digital anarchy, International law, Meta-space, Digital sovereignty, Virtual conflicts, Geneva Conventions.

Məqalənin redaksiyaya daxil olduğu tarix: 03 dekabr 2025-ci il.
Məqalənin çapa qəbul olunma tarixi: 29 yanvar 2026-cı il.
Rəyçilər: t.ü.f.d. Samirə Məmmədova, t.ü.f.d. Məmmədağa Baxışov.