Təcavüz Cinayətinin Törədilməsində Kibergüc Tətbiqi: Kibermüharibələr

Vüqar Qədimov
Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası, Bakı, Azərbaycan
vugargadimov24@gmail.com

***Xülasə*— Müasir dövrdə rəqəmsal texnologiyaların geniş yayılması və süni intellekt sistemlərinin idarə olunması şəraitində təcavüz cinayətinin yeni törədilmə formaları meydana çıxır. Xüsusilə də, kibergüc tətbiqi ilə həyata keçirilən hücumların hüquqi mahiyyəti və onların beynəlxalq cinayət hüququ baxımından qiymətləndirilməsi mühüm əhəmiyyət kəsb edir. Bu tədqiqatda kibermüharibə fəaliyyəti (cyber warfare), onun təcavüz cinayəti ilə əlaqəsi və bu sahədə mövcud olan əsas problemlər və çağırışlar kompleks şəkildə araşdırılır və hüquqi təhlil olunur.**

Açar sözlər*— *təcavüz cinayəti; kibergüc; kiberhücum; kibermüharibə.

I. GİRİŞ

Rəqəmsal texnologiyaların fasiləsiz inkişafı ənənəvi cinayətlərin törədilməsi sahəsində yeni üsulların, xüsusilə də, kiber üsulların meydana çıxmasına səbəb olmuş və beynəlxalq hüququn tətbiqi baxımından yeni çağırışlar yaratmışdır. Bu baxımdan, beynəlxalq cinayətlərin (təcavüz cinayəti, insanlıq əleyhinə cinayətlər, soyqırım və müharibə cinayətləri) kibergüc tətbiqi və kiberəməliyyatların həyata keçirilməsi şəraitində törədilməsi imkanı artıq real hüquqi problem kimi çıxış etməkdədir. Lakin belə əməliyyatların beynəlxalq hüququn konkret prinsiplərinə (məsələn, universallıq prinsipi və s.) əsaslanan cinayətlərin, xüsusilə də, təcavüz cinayətinin tərkib əlaməti kimi çıxış edib-etməməsi məsələsi hələ də tam şəkildə müəyyən edilməmişdir [1].

Təcavüz cinayətinin törədilməsində kibergüc tətbiqi məsələsinə keçməzdən əvvəl beynəlxalq hüquqda "güc" (ing. force) tətbiqini şərtləndirən və onu qadağan edən hallara nəzər salmaq zəruridir. Qeyd edilməlidir ki, qeyri-müəyyən müddətə (müddətsiz) qüvvədə qalması nəzərdə tutulan müqavilələrdə istifadə olunan digər ümumi terminlər kimi "güc" anlayışı da zamanla inkişaf edən və dəyişən məzmuna malikdir.

Güc tətbiqinin həyata keçirilməsi ilə bağlı hallar hələ 28 iyun 1919-cu il tarixli Versal Sülh Müqaviləsinin tərkib hissəsi olan Millətlər Cəmiyyətinin Nizamnaməsində öz əksini tapmışdır. Belə ki, Nizamnamənin 10 və 16-cı maddələrinin mahiyyətinə əsasən əgər üzv dövlətlərdən biri müəyyən edilmiş qaydaları pozaraq müharibəyə başlayarsa, digər üzv dövlətlər dərhal ona qarşı sanksiyalar tətbiq edə, həmçinin Şura tərəfindən tövsiyə olunan hərbi qüvvələrdən istifadə etməklə qaydaları pozan dövlətə qarşı müdaxilə həyata keçirə bilərdilər. Göründüyü kimi, bu halda güc tətbiqi kollektiv şəkildə icazə verilən və qanuni hərbi müdaxilə kimi qiymətləndirilirdi [2].

Dövlətlərarası münaqişələrin həllində güc tətbiqinin və dolayısı ilə dövlət aktı kimi təcavüzün qadağan edilməsi 27 avqust 1928-ci il tarixli Paris Paktında öz əksini tapmışdır. Paris Paktı, eyni zamanda, təcavüzü qeyri-qanuni hesab edən və dövlətlərin milli siyasət aləti kimi müharibədən imtina etməsi üçün beynəlxalq hüquqi öhdəliyi təsbit edən ilk çoxtərəfli aktlardan biri olmuşdur [3].

"Jus ad bellum" sisteminin əsas dayağı olan 26 iyun 1945-ci il tarixli Birləşmiş Millətlər Təşkilatının (BMT) Nizamnaməsinin 2(4)-cü maddəsi və VII Fəsli güc tətbiqini bir daha qadağan etmişdir. Belə ki, Nizamnamənin 2-ci maddəsinin 4-cü bəndində göstərilir: "Bütün üzvlər öz beynəlxalq münasibətlərində hər hansı bir dövlətin ərazi bütövlüyünə və siyasi müstəqilliyinə qarşı və ya BMT-nin məqsədləri ilə ziddiyyət təşkil edən hər hansı bir şəkildə güclə hədələməkdən və güc tətbiq etməkdən çəkinirlər [4]".

Buna uyğun olaraq Azərbaycan Respublikasının 12 noyabr 1995-ci il tarixli Konstitusiyasının 9-cu maddəsinin 2-ci bəndində də qeyd edilmişdir ki, "Azərbaycan Respublikası başqa dövlətlərin müstəqilliyinə qəsd vasitəsi kimi və beynəlxalq münaqişələrin həlli üsulu kimi müharibəni rədd edir [5]".

II. ƏSAS MÜDDƏALAR

Yuxarıda təhlil edilən "güc tətbiqi" anlayışı bir əsrdən artıq müddətdə müasir texnologiyaların inkişafı ilə yeni məna qazanmışdır. Belə ki, BMT-nin Baş Məclisinin 9 sentyabr 2009-cu il tarixli "Beynəlxalq təhlükəsizlik kontekstində informasiya və telekommunikasiya sahəsindəki inkişaflar" mövzusuna həsr olunmuş 64-cü sessiyasında bəzi dövlətlər kritik informasiya infrastrukturunun sıradan çıxarılmasını açıq şəkildə güc tətbiqi kimi qiymətləndirmişlər. Həmin sessiyada Mali Respublikası bəyan etmişdir ki, "İnformasiya silahından istifadə o halda təcavüz aktı kimi şərh oluna bilər ki, zərərçəkmiş dövlətin hücumun başqa bir dövlətin silahlı qüvvələri tərəfindən həyata keçirildiyinə və onun məqsədinin hərbi obyektlərin fəaliyyətini pozmaq, müdafiə və iqtisadi potensialı məhv etmək, yaxud dövlətin müəyyən ərazi üzərində suverenliyini pozmaq olduğuna dair əsaslı səbəbləri olsun [6]".

Təsadüfi deyildir ki, Avropa İttifaqı Şurasının 18 noyabr 2024-cü il tarixli "Kiber məkanında beynəlxalq hüququn ortaq anlaşılması haqqında" Bəyannaməsinin 4-cü bəndində vurğulanır ki, şəraitdən asılı olaraq bir neçə kiberəməliyyatın ümumi təsiri ənənəvi kinetik güc tətbiqi ilə müqayisə oluna bilər. Əgər kiberəməliyyatların miqyası və nəticələri ənənəvi güc tətbiqi ilə müqayisə edilə bilərsə, bu hal BMT Nizamnaməsinin 2-ci maddəsinin 4-cü bəndində nəzərdə

DOI: 10.25045/forensic.gov.2026.92

tutulmuş güc tətbiqi hesab edilir və xüsusi əsaslandırma olmadıqca qadağandır [7].

Bu Bəyannaməyə əsasən belə nəticəyə gəlmək olar ki, "güc tətbiqi" anlayışı geniş mənada "kibergüc tətbiqi"ni də əhatə edə bilər.

Kibergüc tətbiqində digər vacib məqam müdafiə tədbirlərinin həyata keçirilməsində kiberəməliyyatların mümkünlüyü ilə bağlıdır. Məlumdur ki, BMT Nizamnaməsinə uyğun olaraq, hər bir dövlət özünü müdafiə hüququndan istifadə edərək (mad. 51) ərazi bütövlüyünü qorumaq məqsədilə istənilən vaxt fərdi qaydada və ya kollektiv şəkildə (başqa dövlətlərlə birgə) hərbi tədbirlər görə bilər. Həmçinin dövlətlər BMT Təhlükəsizlik Şurasının qərarı ilə koalisiya silahlı qüvvələrinin tərkibində beynəlxalq sülhün və təhlükəsizliyin qorunub saxlanması və ya bərpası üçün hava, dəniz və ya quru qoşunları vasitəsilə zəruri tədbirləri həyata keçirə bilərlər (mad. 42) [8]. Odur ki, kibermüharibə şəraitində dövlətlərə qarşı həyata keçirilən kibergüc tətbiqi çərçivəsindəki kiberhücumların silahlı hücum hesab edilərək özünü müdafiə hüququna əsas verib-verməməsi məsələsi ən çox mübahisəyə açıq mövzulardan biri kimi qalır.

Bunu da qeyd etmək lazımdır ki, BMT Nizamnaməsinin 51-ci maddəsindəki "silahlı hücum" termini "kiberhücum"u əhatə etmir, çünki bu norma tarixi şərh baxımından özündə ənənəvi silahların tətbiqini ehtiva edir. Lakin, Müəllif Ketrin C. Hinklın fikrincə əgər silahlı qüvvələr tərəfindən həyata keçirilirsə, kiberhücumlar silahlı hücum kimi qiymətləndirilə bilər [9].

Müəllifin qeyd edilən yanaşması "silahlı hücum" anlayışının mənasının genişləndirilməsinə əsaslanır və bu yanaşma beynəlxalq hüquq çərçivəsində müəyyən mübahisələr yaradır, çünki kiberhücumların zərərləri hələ də ənənəvi silahlı hücumların kateqoriyasına tam şəkildə daxil edilməmişdir. Bu yanaşmadan yola çıxsaq deyə bilərik ki, BMT Baş Məclisinin 18 noyabr 1987-ci il tarixli "Beynəlxalq münasibətlərdə güc tətbiqindən və təhdidindən çəkinmək prinsipinin effektivliyinin artırılması haqqında" Bəyannamənin 8-ci maddəsində təsbit edilmişdir: "Heç bir dövlət digər dövləti öz suveren hüquqlarının həyata keçirilməsini məhdudlaşdırmaq və ya ondan hər hansı üstünlük əldə etmək üçün iqtisadi, siyasi və ya hər hansı digər vasitələrdən istifadə edə və ya belə istifadəyə təşviq edə bilməz" [10]. Odur ki, "digər vasitələr" ifadəsi də burada geniş şəkildə şərh edilərək kibervasitələri də ehtiva edə bilər.

Beynəlxalq Ədalət Məhkəməsinin presedent hüququ da bu məsələdə olduqca mühüm əhəmiyyət kəsb edir. Belə ki, məşhur *Nicaragua* (Nicaragua v. United States) işində Məhkəmə qərarın 195-ci paraqrafına uyğun olaraq BMT Baş Assambleyasının 1974-cü il tarixli Təcavüzün Tərifinə (xüsusilə 3-cü maddənin (g) bəndinə) istinad edərək qeyd etmişdir ki, hərəkətin silahlı hücum hesab olunub-olunmaması onun miqyası və təsirləri ilə müəyyən edilir. Odur ki, əgər kiberhücumun miqyası və nəticələri (məsələn, elektrik şəbəkəsinin kütləvi sıradan çıxması, insan ölümü və ya fiziki dağıntı) kinetik hücumun nəticələri ilə müqayisə edilə bilirsə, bu, Məhkəmənin Nikaraqua və Amerika Birlıçmiş Ştatları işi üzrə qərarında müəyyən edilmiş silahlı hücum meyarına uyğun hesab oluna bilər [11].

Nəzərə almaq lazımdır ki, Məhkəmə həmin qərarın 228-ci paraqrafında qeyd etmişdir ki, silahlı qrupların silahlandırılması və təlimi birbaşa dağıdıcı hərəkət olmasa da, beynəlxalq hüquq baxımından güc tətbiqi kimi qiymətləndirilə bilər [12].

Başqa bir yanaşmada isə müəlliflərdən A.Maskun və digərləri hesab edirlər ki, fərdi qaydada və ya kollektiv şəkildə həyata keçirilən müdafiə tədbirləri çərçivəsində "qarşı tədbirlər görmək" hər zaman düzgün addım hesab edilə bilməz. Həmçinin, onların fikrincə, belə tədbirlər qarşılıqlı "təzyiq" vasitəsi ilə deyil, "kompensasiya" yolu ilə həyata keçirilməlidir [13].

Buna baxmayaraq, hesab etmək olar ki, bir dövlətin kiberhücumlara cavab olaraq həyata keçirdiyi müdafiə tədbirləri həm BMT Nizamnaməsinin 2(4) maddəsinə, həm də 39, 42 və 51-ci maddələrinə uyğun olaraq qiymətləndirilə bilər. Belə ki, BMT Təhlükəsizlik Şurası 39 və 42-ci maddələr çərçivəsində sülhə təhlükə, sülhün pozulması və ya təcavüz aktı hallarında güc tətbiqinə, o cümlədən kiberəməliyyatlara icazə verə bilər. Hazırda Təhlükəsizlik Şurası heç bir kiberəməliyyatı rəsmi şəkildə bu kateqoriyaya daxil etməsə də, bu səlahiyyət mübahisəsizdir. Təhlükəsizlik Şurası həm konkret hadisələr, həm də ümumi risklər (məsələn, terrorizm və kütləvi qırğın silahlarının yayılması) əsasında sülhə təhlükəni qiymətləndirə bilər. Misal olaraq, kritik informasiya infrastrukturlarına qarşı yönəlmiş kiberəməliyyatlar bu kontekstdə sülhə təhdid hesab edilə bilər.

Odur ki, yuxarıda qeyd edilənləri ümumiləşdirərək, qeyd edə bilərik ki, kiberəməliyyatlar çərçivəsində kibergüc ilə hədələmə, əgər həyata keçirildikdə qanunsuz güc tətbiqi hesab ediləcəksə, güc ilə hədələmə kimi qiymətləndirilə bilər. Eyni zamanda, kibergüc tətbiqi miqyası və nəticələri baxımından ənənəvi silahlı güc tətbiqi səviyyəsinə çatarsa, bu da güc tətbiq etmə kimi qiymətləndirilə bilər.

Təcavüz cinayətinin kibergüc tətbiqi ilə törədilməsini təhlil edərkən, dövlət fəaliyyəti kontekstində "təcavüz aktı"na diqqət yetirmək xüsusilə vacibdir. Belə ki, BMT Baş Məclisinin 14 dekabr 1974-cü il tarixli 3314 (XXIX) saylı Qətnaməsinin 1-ci maddəsində qeyd olunur ki, "təcavüz bir dövlətin digər dövlətin suverenliyi, ərazi bütövlüyü və ya siyasi müstəqilliyi əleyhinə və ya bu tərifdə müəyyən olunduğu kimi, BMT Nizamnaməsi ilə uzlaşmayan şəkildə silahlı güc tətbiq etməsidir". Nəzərə almaq lazımdır ki, burada məsuliyyətin subyekti kimi dövlətlər çıxış edir [14].

Dövlətlərin beynəlxalq hüquqa zidd əməllərinə görə məsuliyyət məsələsinin ümumi hüquqi çərçivəsi də bu kontekstdə nəzərə alınmalıdır [15]. Bu Qətnamənin 3-cü maddəsində "təcavüz aktı" kimi qiymətləndirilən dairəsi müəyyən edilmişdir. Qəbul edildiyi dövr və tarixi-siyasi şərait nəzərə alınaraq, bu əməllərin fiziki güc tətbiqini özündə ehtiva edir. Lakin, bəzi müəlliflər hesab edir ki, burada təsbit edilən əməllər müasir dövrün obyektiv gerçəkliyinə uyğun şəkildə geniş şərh edilə bilər. Belə ki, müəlliflərdən M.Roscini hesab edir ki, bir dövlət bilə-bilə digər dövlətin öz kiber infrastrukturundan istifadə edərək üçüncü bir dövlətə qarşı təcavüz aktı təşkil edən kiberhücum həyata keçirməsinə imkan verərsə, o zaman həmin dövlət özü də təcavüz aktı törətmiş

sayılacaq və buna görə güc tətbiqinin qadağanını pozmuş olacaqdır [16].

Bununla belə, Qətnamənin 4-cü maddəsində göstərilir ki, əvvəlki maddədə sadalanan əməllər tam siyahı təşkil etmir və Təhlükəsizlik Şurası Nizamnamənin müddəalarına əsaslanaraq digər aktların da təcavüz aktı olduğunu müəyyən edə bilər [17]. Beləliklə, kiberəməliyyatların təcavüz aktı kimi qiymətləndirilməsi məsələsi Təhlükəsizlik Şurasının müstəsna səlahiyyəti çərçivəsində həm nəzəri, həm də praktik olaraq mümkün olması bir daha öz əksini tapır.

Bir məsələyə də aydınlıq gətirmək lazımdır ki, təcavüz aktının həyata keçirilməsi həmişə silahlı güc tətbiqi ilə kibergüc tətbiqinin birgə baş verməsini tələb etmir [1]. Yəni, kibergüc tətbiqi həm silahlı güc ilə birlikdə, həm də müstəqil kateqoriya kimi qiymətləndirilməlidir. Lakin qeyd etmək vacibdir ki, kibergüc tətbiqi hər zaman təcavüz aktı hesab edilməyə və kibermüharibəyə səbəb olmaya bilər. M.Robinson və digər müəlliflər haqlı olaraq "kibermüharibə fəaliyyəti (cyber warfare)" və "kibermüharibə (cyber war)" terminlərini fərqləndirirlər [18].

Belə ki, "kibermüharibə fəaliyyəti" dedikdə, kiberhücumlarla həyata keçirilən və müharibəyə bənzər fəaliyyət başa düşülür. Yəni, bu halda dövlət hələ rəsmi müharibə elan etməyə də bilər (və ya ənənəvi müharibə çərçivəsində kibermüharibə əməliyyatları da aparıla bilər) [18].

Bundan fərqli olaraq, "kibermüharibə" yalnız rəsmi elan edilmiş və yalnız kiberhücumlar vasitəsilə aparılan müharibə sayılır. Əgər bu zaman ənənəvi hərbi güc tətbiq olunarsa, belə vəziyyət sadəcə müharibə (ing. war) hesab ediləcəkdir.

Kibergüc tətbiqi və kibermüharibələrə dair yanaşmalar, təcavüz aktına verilən tərifdə "suverenlik, ərazi bütövlüyü və siyasi müstəqillik" anlayışlarının kiberməkan kontekstində açıqlanmasını zəruri edir. Doğrudur, bunların təhlili başqa bir tədqiqatın mövzusu olsa da, müəlliflərdən V.H. fon Hayneq yanaşmasını qeyd etməyi zəruri hesab edirik. Müəllif qeyd edir ki, ərazi suverenliyi beynəlxalq hüququn güclü və təsirli normalarından biridir və əgər kiberməkan dövlətin ərazisində yerləşən və ya ərazi suverenliyi prinsipi ilə qorunan komponentlərdən, yəni kiber infrastrukturdan ibarət kimi qəbul 9edilərsə, bu norma kiberməkana da tətbiq oluna bilər [19].

Habelə, kiberməkanı geniş şəkildə qiymətləndirən müəlliflərdən R.S.Oqbe bildirir ki, kiberhücumların arxasında duran texnoloji sistemlər və şəbəkələr çox mürəkkəbdir. Buna görə də, kiberhücum yalnız hücum edilən ölkədəki şəxslərə deyil, dünyanın digər yerlərindəki hədəf şəxslərə də təsir göstərə bilər. Yəni, hədəf fiziki olaraq hücum edilən ölkədə olmasa belə, kiberməkanın qlobal və əlaqəli təbiəti səbəbindən hücumdan zərər görə bilər [20].

Beynəlxalq cinayət kimi təcavüz cinayətinin törədilməsində kiberhücumların cinayətin elementi kimi qiymətləndirilməsi Beynəlxalq Cinayət Məhkəməsinin yurisdiksiyası üzrə xüsusi əhəmiyyət daşıyır. 17 iyul 1998-ci il tarixində qəbul edilmiş Roma Statutu ilə beynəlxalq ictimaiyyəti narahat edən ən ağır cinayətləri törətməkdə ittiham olunan şəxslərin mühakimə olunması məqsədilə daimi beynəlxalq məhkəmə təsis edilmişdir [21].

Lakin təcavüz cinayəti üzrə fərdi cinayət məsuliyyəti ilə bağlı məhkəmənin yurisdiksiyası 31 may-11 iyun 2010-cu il tarixlərində Uqandanın paytaxtı Kampalada keçirilmiş İcmal Konfransına qədər açıq qalmışdır.

Konfransın yekunundan sonra Tərəf Dövlətlər Məclisi Kampala İcmal Konfransında təcavüz cinayətini faktiki olaraq tətbiq edilə bilən hala gətirdi. Belə ki, Roma Statutuna 8 bis maddəsi əlavə olunaraq təcavüz cinayətinə hüquqi tərif verildi. 15 bis və 15 ter maddələri ilə cinayət-hüquqi yurisdiksiya şərtləri müəyyən edildi. Bu cinayət üzrə yurisdiksiya yalnız 1 yanvar 2017-ci ildən sonra (rəsmi olaraq 17 iyul 2018-ci ildən etibarən) və ən azı 30 dövlətin ratifikasiyasından sonra aktivləşə bilərdi. Qeyri-üzv dövlətlərə qarşı yurisdiksiya yalnız BMT Təhlükəsizlik Şurasının göndərişi ilə mümkün idi. Üzv dövlətlər üçün isə "opt-out" mexanizmi nəzərdə tutulmuşdur (15 bis-4). Təhlükəsizlik Şurası altı ay ərzində qərar verməzsə, Prokuror Beynəlxalq Cinayət Məhkəməsinin (BCM) icazəsi ilə istintaqa başlaya bilərdi [21].

Uzun illər ərzində Beynəlxalq Cinayət Məhkəməsinin təcavüz cinayəti üzrə yurisdiksiyası "siyasi xarakterli" hesab edilmiş və bu səbəbdən ciddi tənqidlərə məruz qalmışdır. Təsadüfi deyildir ki, 4 aprel 2025-ci il tarixində bir sıra Tərəf Dövlətlər, o cümlədən Kosta Rika, Almaniya və Syerra-Leone və s. təcavüz cinayəti üzrə yurisdiksiyanın digər beynəlxalq cinayətlərin yurisdiksiyası ilə uyğunlaşdırılması məqsədilə harmonizasiya xarakterli dəyişiklik təklifi irəli sürmüşlər [22].

III. BCM KONTEKSTİNDƏ

Müasir dövrdə ənənəvi cinayətkarlığın törədilmə formalarına kiber üsulların tətbiqi Beynəlxalq Cinayət Məhkəməsinin yurisdiksiyasına daxil olan cinayətlərə münasibətdə mövqeyini ifadə etməsini zəruri etmişdir. Bu baxımdan BCM-in Prokurorluq İdarəsinin 2 dekabr 2025-ci il tarixli "Kiber əsaslı cinayətlərə dair siyasət" sənədində "kiber" terminina anlayış verilmişdir. Həmin sənəddə "kiber" termini informasiya və kommunikasiya texnologiyalarını (İKT), şəbəkələri və süni intellekti (AI) əhatə edən fəaliyyətlərin geniş spektrini ifadə edir.

Dərc edilmiş bu sənəddə kiber üsullarla törədilə bilən cinayətlərin dairəsi də müəyyən edilmişdir. Sənəddə qeyd olunur ki, Beynəlxalq Cinayət Məhkəməsinin yurisdiksiyasına daxil olan soyqırım, insanlıq əleyhinə cinayətlər, müharibə cinayətləri və təcavüz cinayəti, habelə ədalət mühakiməsi əleyhinə olan cinayətlər (Cinayət Məcəlləsinin 32-ci Fəsli kontekstində [23] (məsələn, sübutların saxtalaşdırılması və s.) kiber üsullarla törədilə bilər. Bu baxımdan "kiber" termini həmin cinayətlərin ayrıca yeni növünü deyil, əksinə, Məhkəmənin yurisdiksiyasına daxil olan mövcud beynəlxalq cinayətlərin (ədalət mühakiməsi əleyhinə olan cinayətlər də daxil olmaqla) birbaşa və ya dolayı şəkildə kiber vasitələrlə törədilə bilməsini ifadə edən funksional anlayış kimi istifadə olunur [24].

Bununla belə, Beynəlxalq Cinayət Məhkəməsi qeyd etmişdir ki, təcavüz cinayəti ilə bağlı bu günədək hər hansı icraatın aparılmaması həmin məsələnin daha məhdud şəkildə şərh edilməsini zəruri edir. Lakin bu yanaşma ümumi tendensiyadan kənar qiymətləndirilməməlidir.

Təcavüz cinayətinin kiber üsulla törədilməsinin özünəməxsus xüsusiyyətlərinin təhlilinə keçməzdən qabaq onun BCM-in Roma Statutunda nəzərdə tutulmuş anlayışına nəzər salmaq zəruridir. Roma Statutunun 8 bis (1)-ci maddəsinə əsasən, təcavüz cinayəti bir şəxsin dövlətin siyasi və ya hərbi fəaliyyətinə effektiv nəzarət etmək və ya onu istiqamətləndirmək səlahiyyətinə malik olduğu halda təcavüz aktını planlaşdırması, hazırlaması, başlaması və ya aparması ilə xarakterizə olunur; belə akt öz xarakteri, ağırlığı və miqyası etibarilə Birləşmiş Millətlər Təşkilatının Nizamnaməsinin açıq pozuntusunu təşkil etməlidir. Həmçinin, Statutun 8 bis (2)-ci maddəsinə görə təcavüz aktı bir dövlət tərəfindən digər bir dövlətin suverenliyinə, ərazi bütövlüyünə və ya siyasi müstəqilliyinə qarşı silahlı qüvvədən istifadə, yaxud BMT Nizamnaməsinə uyğun olmayan hər hansı digər davranış kimi müəyyən edilir. Həmin maddədə belə aktlara nümunə olaraq işğal, bombardman və bir dövlətin silahlı qüvvələrinin digər bir dövlətin silahlı qüvvələrinə hücumu göstərilir [24].

Odur ki, Roma Statutunda təcavüz cinayətini şərtləndirən əməllər əsasən ənənəvi törədilmə formalarını əks etdirir. Bununla belə, Beynəlxalq Cinayət Məhkəməsinin Prokurorluq İdarəsi qeyd edir ki, müəyyən hallarda kiber əməliyyat da Birləşmiş Millətlər Təşkilatının Nizamnaməsinin 2(4)-cü maddəsi ilə qadağan olunmuş güc tətbiqi və nəticə etibarilə təcavüz aktı kimi qiymətləndirilə bilər. Bu kontekstdə həlledici meyar istifadə olunan texnoloji vasitələr (kiber üsullar) deyil, konkret hərəkətin gücdən istifadə kimi qiymətləndirilməsinə əsas verən nəticələrdir. Məsələn, bir dövlətin operatorları digər dövlətin silahlı qüvvələrinə qarşı kiberəməliyyat həyata keçirərək hərbi təyyarələrin və ya gəmilərin naviqasiya sistemlərinə müdaxilə edə və bunun nəticəsində ölüm, xəsarət və ya ciddi maddi zərər yarada bilər [25].

Digər tərəfdən, təcavüz aktının Birləşmiş Millətlər Təşkilatının Nizamnaməsinin "açıq pozuntusu" təşkil edib-etmədiyi onun "xarakteri, ağırlığı və miqyası" kimi meyarları əsasında müəyyən edilir. Bu amilləri qiymətləndirərkən Beynəlxalq Cinayət Məhkəməsinin Prokurorluq İdarəsi digər hallarla yanaşı, təcavüz aktının yaratdığı fiziki ziyanı, o cümlədən təbii mühitə vurulan ziyanı, habelə qurbanların sayını və xarakterini nəzərə alacağını qeyd edir. Siyasət sənədində bu da qeyd olunur ki, təcavüz cinayətinin yalnız kiber üsulla törədilməsi nəzəri baxımdan mümkün olsa da, praktik baxımdan daha çox ehtimal olunur ki, kiberəməliyyatlar təcavüzkar dövlət tərəfindən daha geniş fəaliyyət planının tərkib hissəsi kimi istifadə olunsun və bu plan çərçivəsində fiziki və ya kinetik qüvvənin tətbiqini nəzərdə tutan hərəkətlər də yer alsın [25].

Bu baxımdan BCM-in Prokurorluq İdarəsi təcavüz kampaniyasının bütün elementlərinin xarakterini, ağırlığını və miqyasını kompleks (holistik) şəkildə qiymətləndirəcəyini və kiberməkanda həyata keçirilən hərəkətləri ayrı-ayrılıqda deyil, ümumi fəaliyyət kontekstində nəzərdən keçirəcəyini vurğulayır.

Odur ki, qeyd edilən siyasət sənədində BCM-in Prokurorluq İdarəsi təcavüz cinayətinin törədilməsi zamanı kibermüharibə fəaliyyəti şəraitində kibergüc tətbiqinin hüquqi baxımdan mümkünlüyünü faktiki olaraq qəbul etdiyini ifadə edir.

Təcavüz cinayətinin kiber üsulla törədilməsində dövlətin haker qruplarından və ya proksi qüvvələrdən istifadəsi də təcavüz cinayətinin törədilməsi konteksində qiymətləndirilə bilər. Bu zaman rəhbər şəxsin bu qüvvələrdən istifadəyə dair obyektiv (planlama, hazırlama, başlama və ya aparma), eləcə də subyektiv əlamətlər (təqsir, niyyət) birgə nəzərə alınmalıdır [26].

Digər tərəfdən, məlumdur ki, təcavüz cinayəti Roma Statutunda digər beynəlxalq cinayətlərdən fərqlənir, çünki bu cinayət yalnız siyasi və ya hərbi rəhbərin dövlət fəaliyyətini nəzarətdə saxlaya və ya onu yönəldə bilməsi halında törədilə bilər. Lakin kibermüharibə fəaliyyəti şəraitində rəhbərliyə xas yuxarıdakı tələbin birbaşa tətbiqi istisna edilə bilər [26].

NƏTİCƏ

Yuxarıda qeyd edilənlərə əsasən deyə bilərik ki, müasir dövrdə kibergüc tətbiqi, əgər nəticələri və miqyası ənənəvi silahlı güc tətbiqi ilə müqayisə olunarsa, kibermüharibə fəaliyyəti şəraitində təcavüz aktı və ya güc tətbiqi ilə birgə və ya kibermüharibə şəraitində müstəqil kateqoriya (kibergüc tətbiqi) kimi qiymətləndirilə bilər.

Eyni zamanda, Roma Statutu çərçivəsində kiber üsulla törədilən təcavüz cinayətinə görə fərdi məsuliyyət BCM-in Prokurorluq İdarəsinin müəyyən etdiyi siyasət şərtləri ilə mümkündür.

Dövlətlər kibermüharibə fəaliyyəti şəraitində özünü müdafiə hüququndan istifadə edə bilər, lakin bu hüquq BMT Nizamnaməsinin müddəalarına və Təhlükəsizlik Şurasının qərarına əsaslanmalıdır.

ƏDƏBİYYAT

[1] M. N. Schmitt, Ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, UK: Cambridge University Press, 2017.

[2] The Covenant of the League of Nations, League of Nations, Apr. 28, 1919.

[3] Sh. T. Samedova, Ugolovnoe Pravo Azerbaidzhanskoi Respubliki. Osobennaya Chast [Criminal Law of the Republic of Azerbaijan. Special Part], 2 parts. Baku, Azerbaijan: Adiloglu, 2020, vol. 1.

[4] United Nations Charter, San Francisco, CA, USA, June 26, 1945.

[5] Azərbaycan Respublikasının Konstitusiyası [Constitution of the Republic of Azerbaijan]. Baku, Azerbaijan: Hüquq Yayın Evi, 2025.

[6] UN General Assembly, "Developments in the field of information and telecommunications in the context of international security," Report of the Secretary-General, A/64/129/Add.1, Sep. 9, 2009.

[7] Council of the European Union, "Declaration on a common understanding of international law in cyberspace," Brussels, Belgium, Nov. 18, 2024.

[8] Ş. T. Səmədova, Transmilli Cinayət Hüququnun Nəzəri və Praktiki Problemləri [Theoretical and Practical Problems of Transnational Criminal Law]. Baku, Azerbaijan: Mütərcim, 2023.

[9] K. C. Hinkle, "Countermeasures in the cyber context: One more thing to worry about," Yale Journal of International Law, vol. 37, pp. 11–21, 2010.

[10] UN General Assembly, "Declaration on the enhancement of the effectiveness of the principle of refraining from the threat or use of force in international relations," Resolution 42/22, New York, NY, USA, 1987.

[11] "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)," ICJ Reports, pp. 195, 228, 1986.

[12] E. Əliyev, "Beynəlxalq hüquqda təcavüzə görə dövlətlərin məsuliyyəti," Polis Akademiyasının Elmi Xəbərləri, no. 3 (35), 2022.

[13] A. Maskun, H. A. Naswar, S. Armelia, M. Napang, and M. Hendrapati, "Qualifying cyber crime as a crime of aggression in international law," Journal of East Asia and International Law, vol. 13, no. 2, pp. 397–418, 2020.

[14] UN General Assembly, "Definition of aggression," Resolution 3314 (XXIX), New York, NY, USA, Dec. 14, 1974.

[15] J. Crawford, The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries. Cambridge, UK: Cambridge University Press, 2002.

[16] M. Roscini, Cyber Operations and the Use of Force in International Law. Oxford, UK: Oxford University Press, 2014.

[17] UN General Assembly, "Definition of aggression," Resolution 3314 (XXIX), New York, NY, USA, Dec. 14, 1974.

[18] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," Computers & Security, vol. 49, pp. 70–94, 2015.

[19] W. H. von Heinegg, "Legal implications of territorial sovereignty in cyberspace," Faculty of Law, Europa-Universität Viadrina, Frankfurt (Oder), Germany, Research Paper, 2012.

[20] R. S. Ogbe, "International law, cyber crime and crime of aggression," African Journal of Criminal Law and Jurisprudence, vol. 8, 2023.

[21] D. Tezcan, M. R. Erdem, and R. M. Önok, Uluslararası Ceza Hukuku [International Criminal Law], 6th ed. Ankara, Turkey: Seçkin Hukuk, 2021.

[22] Costa Rica, Germany, Sierra Leone, Slovenia, and Vanuatu, "Proposal of amendment (Annex)," United Nations, Depositary Notification C.N.162.2025.TREATIES-XVIII.10, Apr. 4, 2025.

[23] Azərbaycan Respublikasının Cinayət Məcəlləsi. Baku, Azerbaijan: Qanun Nəşriyyatı, 2025.

[24] Rome Statute of the International Criminal Court, United Nations, July 17, 1998.

[25] Policy on Cyber-Enabled Crimes under the Rome Statute, International Criminal Court (ICC), The Hague, Netherlands, 2025.

[26] Elements of Crimes, United Nations, New York, NY, USA, 2002; Amendments: Review Conference Records, Kampala, 2010.

Use of Cyber Force in the Commission of the Crime of Aggression: Cyber War

Vugar Gadimov
Heydar Aliyev Academy of the State Security Service,
Baku, Azerbaijan
vugargadimov24@gmail.com

Abstract- In the modern era, characterized by the widespread use of digital technologies and the governance of artificial intelligence systems, new forms of committing the crime of aggression are emerging. In particular, the legal nature of attacks carried out through the use of cyber force and their assessment from the perspective of international criminal law are of significant importance. This study comprehensively examines cyber warfare activity (cyber warfare), its relationship with the crime of aggression, as well as the main challenges and issues existing in this field, and provides a legal analysis thereof.

Keyword- crime of aggression; cyberforce; cyberattack; cyber warfare