Mehdi Abdullayev. Kiberhücumların silahlı münaqişə kimi qiymətləndirilməsi: beynəlxalq hüquq normaları əsasında araşdırma // Azərbaycan Hüquq Jurnalı. 2025 (№3), s. 28-37.
DOI: 10.61638/KQRM1533

BEYNƏLXALQ CİNAYƏT HÜQUQU

KİBERHÜCUMLARIN SİLAHLI MÜNAQİŞƏ KİMİ QİYMƏTLƏNDİRİLMƏSİ: BEYNƏLXALQ HÜQUQ NORMALARI ƏSASINDA ARAŞDIRMA

MEHDİ ABDULLAYEV*

Annotasiya

Məqalədə kiberhücumların silahlı münaqişə kimi qiymətləndirilməsi beynəlxalq hüquq normaları əsasında (BMT Nizamnaməsi, Müharibə qurbanlarının müdafiəsi haqqında Cenevrə Konvensiyaları və Əlavə Protokollar, Tallin Təlimatları və s.) təhlil edilir. Məlum olduğu kimi, beynəlxalq hüquqi tənzimləmənin əsas məqsədini BMT Nizamnaməsində nəzərdə tutulduğu kimi, beynəlxalq sülhü və təhlükəsizliyi təmin etmək təşkil edir. Müasir cəmiyyətin rəqəmsallaşması, kiberməkanın sərhədlərinin bəlli olmaması bu məqsədin yerinə yetirilməsində tamamilə yeni məsələləri gündəmə gətirir. Belə ki, kiberməkanda törədilən hər hansı bir kiberhücumla nəinki bir dövlətə, hətta eyni anda bir neçə dövlətə müxtəlif iqtisadi, siyasi və digər ziyan vurmaq mümkündür. Bu gün hər hansı bir dövlətin kritik informasiya infrastrukturuna yönəlmiş kiberhücumla həmin dövlətin fəaliyyətini "iflic" etmək çox asan və rahat idarə olunan qanunsuz fəaliyyətə çevrilmişdir. Hazırda isə bu təhlükələr daha da artmaqdadır. Təqdim olunan məqalənin başlıca məqsədi kiberhücumlar zamanı beynəlxalq hüququn üzləşdiyi çətinliklərə həll yolu təklif etməkdir. Bu məqsədlə kiberhücumların və kiberhücumçuların anlayışı və əsas xüsusiyyətləri araşdırılmış, beynəlxalq sənədlər əsasında kiberhücumun silahlı münaqişə kimi qiymətləndirilməsi mümkünlüyü tədqiq olunmuşdur. Eyni zamanda, bir sıra mühüm beynəlxalq sənədlərin müddəalarına və beynəlxalq təşkilatların rəylərinə ("bərk" və "yumşaq" hüquq normaları) müqayisəli formada müraciət edilmişdir. Araşdırmanın sonunda kiberhücumların özünün də düşmənçilik xarakteri daşıyan davranış olması nəticəsinə gəlinərək, onların silahlı münaqişələr qədər təhlükəli olması və dövlətlərin bu cür hücumlardan özünümüdafiə hüququna malik olması irəli sürülmüşdür.

Açar sözlər: *kiberməkan, kiberhücum, silahlı münaqişə, silahlı hücum, özünümüdafiə hüququ, kiberəməliyyat, kibercasusluq, kiberaktivizm, BMT Nizamnaməsi, Tallin Təlimatı.*

I. Giriş

Nəhəng texnoloji təhlükəsizlik şirkətlərindən olan Kasperskinin məlumatına görə, qlobal kibertəhdidlər sürətlə inkişaf etməyə davam edir və hər il məlumat sızmalarının sayı artır. RiskBased Security-in hesabatında deyilir ki,

* Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akaddemiyası hüquq elmləri doktoru / email: mehdi.k.abdullayev@gmail.com

təkcə 2019-cu ilin ilk doqquz ayında məlumat sızmaları nəticəsində şokedici 7,9 milyard qeyd aşkar edilmişdir. Bu rəqəm 2018-ci ilin eyni dövründə aşkarlanan qeydlərin sayından iki dəfədən çoxdur (112%) [5].

Kibertəhdidin miqyasının artmağa davam etməsi ilə kibertəhlükəsizlik həllərinə qlobal xərclər təbii olaraq artır. Gartner kibertəhlükəsizlik xərclərinin 2023-cü ildə 188,3 milyard dollara çatacağını və 2026-cı ilə qədər qlobal miqyasda 260 milyard dolları keçəcəyini proqnozlaşdırır. Dünyanın hər yerində dövlətlər artan kibertəhdidlərə təşkilatlara səmərəli kibertəhlükəsizlik təcrübələrini tətbiq etməyə kömək etmək üçün tədbirlər görməkdə davam edirlər. Məsələn, ABŞ-da Milli Standartlar və Texnologiya İnstitutu (NIST) kibertəhlükəsizlik çərçivəsi yaratmışdır. Zərərli kodun yayılmasının qarşısını almaq və erkən aşkarlanmasına kömək etmək üçün çərçivə bütün elektron resursların davamlı, real vaxt rejimində monitorinqini tövsiyə edir [10]. Sistem monitorinqinin əhəmiyyəti Böyük Britaniya hökumətinin Milli Kiber Təhlükəsizlik Mərkəzi tərəfindən təqdim edilən "Kibertəhlükəsizliyə 10 addım" təlimatında öz əksini tapır [1]. Avstraliyada Avstraliya Kiber Təhlükəsizlik Mərkəzi (ACSC) təşkilatların ən son kibertəhlükəsizlik təhdidlərinə necə qarşı çıxa biləcəyi barədə müntəzəm olaraq təlimatlar dərc edir [9]. Respublikamızda bununla bağlı Azərbaycan Respublikasının Milli Kibertəhlükəsizlik Mərkəzi [6] uğurla öz fəaliyyətini davam etdirir. Lakin kibertəhdidlərin daim artması və kiberhücumlar zamanı tətbiq olunan üsul və metodların yenilənməsi kibertəhlükəsizlik strategiyalarının operativliyini və davamlılığını tələb edir. Kibertəhlükəsizlik sahəsində tədbirlərin sayı artsa da, kiberhücumlar dövrümüzün ən böyük probleminə çevrilmişdir. Artıq bu hücumların təhlükəsi o həddə çatmışdır ki, onların silahlı hücum kimi qiymətləndirilməsi ilə bağlı tənzimləmələr aparılmaqdadır.

II. Kiberhücumların anlayışı

İnformasiya Texnologiyaları Sistemləri (İT Sistemləri) bu gün nadir hallarda təcrid olunmuş şəkildə istifadə olunur; onlar adətən qlobal şəbəkəyə qoşulur. İT sistemləri arasında ünsiyyət ümumiyyətlə yerli və qlobal şəbəkələr, məsələn, İnternet və ya mobil radio şəbəkələri vasitəsilə baş verir. Məlumat şəbəkəsinə daim qoşulmayan demək olar ki, bütün kompüterlər zaman-zaman yeni məlumatlarla təmin olunur, məsələn, məlumat daşıyıcısından istifadə edərək yeni məlumat ehtiyatları və ya yeni proqram versiyaları idxal edildikdə. Daha əvvəl qeyd etdiyimiz kimi, qlobal miqyasda əlaqə quran bütün bu İT sistemləri kiberməkan adlanır. Getdikcə daha çox İT rabitə əlaqələrinin dəyişdiyi İnternet kiberməkanın əhəmiyyətli bir hissəsidir. Bununla belə, bir çox digər şəbəkə strukturları da dünya miqyasında geniş istifadə olunur. Buna baxmayaraq, qlobal şəbəkələrin imkanlarından da cinayətkarlar tərəfindən zərərli fəaliyyətlər üçün sui-istifadə olunur. Kiberhücum, kiberməkan əsas hücum vasitəsi kimi istifadə edildikdə və ya özü hücumun hədəfi olduqda baş verir. Çoxsaylı müxtəlif hücum hədəflərinə və potensial hücum metodlarına baxmayaraq, kiberhücumun

arxasındakı motivasiya çox vaxt pul, məlumat toplamaq, təxribatdan tutmuş siyasi maraqlara təsir etmək və ya onları müdafiə etmək qədər dəyişə bilər.

Kiberməkanda qəsdən hərəkət edən hücumçuları aşağıdakı qruplara bölmək olar:

Kiberfəallar. Bunlar kiberhücumlardan siyasi, sosial, iqtisadi və ya texniki idarəetmənin pozulmasına diqqət çəkmək və ya bu məsələyə tələbi gücləndirmək üçün istifadə edən hücumçulardır (haktivizm). Hücumun arxasındakı motivasiya təsirlidir. Kiberhücumun vurduğu zərər etiraf edilir və ya daha çox diqqəti cəlb etməyə məcbur edilir. Sosial məsələlərə diqqət yetirən hakerlər qrupu sözdə etik hakerlərdir (xeyirxah hakerlər). Bu aktivizm forması 1990-cı illərin əvvəllərindən bəri inkişaf etmiş, əvvəlcə e-poçt və mesaj lövhələrinin artması ilə məşhurluq qazanmış, daha sonra isə sosial media və video paylaşma saytları vasitəsilə genişlənmişdir. Əsas fəaliyyətlərə ianə toplama, tədbirlərin təşkili və bloqlar, podkastlar və e-poçt kampaniyaları vasitəsilə maarifləndirmənin yayılması daxildir. Kiberaktivizmdəki əhəmiyyətli mərhələlərə 2000-ci il ABŞ prezident seçkilərindən sonra VoterMarch-ın səfərbərlik səyləri və Facebook və Twitter kimi platformaların real vaxt rejimində etirazların təşkilində və təcrübələrin paylaşılmasında əsas rol oynadığı Ərəb Baharı zamanı sosial medianın geniş istifadəsi daxildir [4].

Kibercinayətkarlar. Kibercinayətkarların motivasiyası informasiya texnologiyalarından istifadə edərək qanunsuz olaraq pul qazanmaqdır. Spektr mütəşəkkil kibercinayətkarlıqdan az zərərli sadə cinayətkarlığa qədər dəyişir. Kibercinayətkarların bir növü də kiberterrorçulardır ki, onlar müxtəlif hədəflərə hücum etmək üçün kiberhücumlardan istifadə edə və bununla da ideologiyalarını yaya və təsirlərini artıra bilərlər.

Kiberməkanda iqtisadi və siyasi casuslar. İnternetin üstünlükləri casuslar üçün yeni imkanlar yaradır. Sənaye casusluğu və rəqabətli casusluq maliyyə maraqlarına xidmət edir. Rəqiblər və onların məhsulları haqqında daxili məlumatlar qlobal rəqabətdə maliyyə üstünlükləri təmin edir. İqtisadi casusluqdan fərqli olaraq, dövlət kəşfiyyat xidmətlərinin kiberhücumları əsasən sırf maliyyə maraqlarından daha çox məlumat toplamağa və təsir göstərməyə xidmət edir.

III. Kiberhücumların silahlı münaqişə kimi qiymətləndirilməsi

Kiberhücumun silahlı münaqişə kimi qiymətləndirilməsi məsələsi son dövrlərin aktual problemlərindən biridir. Əsas qarşıya qoyulan sual bu cür hücumların silahlı münaqişə üçün müəyyən olunmuş meyarlara cavab verib-verməməsidir. Qeyd etməliyik ki, uzun müddət silahlı münaqişənin mövcudluğu müharibə elan edilməsi və ya müharibə vəziyyətinin tanınması kimi formal meyarların təsdiqlənməsi ilə şərtlənirdi. 1949-cu il tarixli Müharibə qurbanlarının müdafiəsi haqqında Birinci Cenevrə Konvensiyasının 2-ci maddəsinin təfsirinə əsasən, silahlı münaqişə silahlı qüvvələr üzvlərinin müdaxiləsinə səbəb olan iki dövlət arasında hər hansı bir mübahisə kimi müəyyən edilir [2]. Silahlı münaqişənin mövcudluğu beynəlxalq humanitar hüququn tətbiqini zəruri edir. Daha dəqiq desək, beynəlxalq humanitar hüquq münaqişədə müharibə edən tərəflər arasında hərbi

əməliyyatların aparılmasını tənzimləyir. Cenevrə Konvensiyalarına Əlavə Protokol I-nin 49-cu maddəsinə görə, təcavüz (hücum) düşmənə qarşı hücum və ya müdafiə məqsədləri üçün zorakılıq aktı kimi müəyyən edilir. Əlavə Protokol I-nin 48-ci maddəsindəki izahata görə, əməliyyat dedikdə, zorakılığın istifadə edildiyi hərbi əməliyyatlar başa düşülür. Protokolun hücumlarla bağlı müddəaları münaqişə tərəfinə məxsus olan, lakin qarşı tərəfin nəzarəti altında olan milli ərazi də daxil olmaqla, aparılan istənilən ərazidə baş verən bütün hücumlara şamil edilir. Sadəcə olaraq, bu maddədəki "hər hansı quru, hava və ya dəniz müharibəsi" ifadəsi kibermüharibəni ehtiva edə bilərmi? – Cenevrə Konvensiyaları və Protokollarından çıxış etsək, bu sənədlər qeyri-kinetik əməliyyatları istisna edir. Təcavüz anlayışına təbliğat əməliyyatları, embarqolar və ya digər iqtisadi və ya psixoloji müharibə vasitələri daxil deyil. Belə olduğu təqdirdə, kiberhücumlar beynəlxalq hüququn əhatə dairəsindən çıxarılmalıdırmı? – Əslində, bu sualın cavablandırılması üçün silahlı münaqişəyə dair meyarlar tam nəzərdən keçirilməlidir.

Ümumilikdə, beynəlxalq humanitar hüquq əhalini və mülki obyektləri qorumağı hədəflədiyindən, burada əməliyyatların mülki əhaliyə təsirindən asılı olaraq, kinetik olub-olmamasından asılı olaraq nəticəyə yönəlmiş yanaşma tətbiq edilməlidir. Buna görə də, bu təfsir yeni deyil, çünki kimyəvi və ya bioloji silahların istifadəsi zərərli nəticələrinə görə həmişə kinetik olmasa belə, hücum hesab edilmişdir. Eynilə, kiberhücum təbiətcə zorakı olmasa belə, ağır nəticələrinə görə hücum və ya düşmənçilik aktı kimi təsnif edilə bilər. Məsələn, böyük bir hava limanında hava nəqliyyatının idarəetmə sisteminə edilən kiberhücum beynəlxalq humanitar hüquqa tabe olardı. Əksinə, universitetə və ya ticarət mərkəzinin veb-saytına hücum beynəlxalq hüququn pozulması adlandırılmaq üçün kifayət etməzdi. Bəs sadəcə bir obyektin funksiyasını pozan və görünən fiziki zərər vermədən zərər verməyən kiberəməliyyatlar "düşmən davranışı" kimi qiymətləndirilə bilərmi? – Qeyd etməliyik ki, hələ 2019-cu ildə Beynəlxalq Qızıl Xaç Komitəsi bu kimi məsələlərlə bağlı öz münasibətini bildirmişdir. Belə ki, "Silahlı münaqişələr zamanı beynəlxalq humanitar hüquq və kiberəməliyyatlar" adlı mövqe sənədində [3] qeyd olunur ki, silahlı münaqişə zamanı kiber əməliyyatların istifadəsi digər müharibə vasitələri və ya metodlarının təklif etmədiyi alternativlər təklif edə bilər, lakin eyni zamanda risklər də daşıyır. Bir tərəfdən, kiberəməliyyatlar silahlı münaqişə tərəflərinə mülki şəxslərə zərər vermədən və ya mülki infrastruktura fiziki ziyan vurmadan hərbi məqsədlərinə çatmaq imkanı vermək potensialına malikdir. Digər tərəfdən, əsasən silahlı münaqişə kontekstindən kənarda aparılan son kiberəməliyyatlar göstərir ki, təcrübəli subyektlər mülki əhaliyə vacib xidmətlərin göstərilməsini pozmaq qabiliyyətini inkişaf etdirmişlər. Kiberəməliyyatlar vasitəsilə müharibə edən tərəflərin sistemə daxil olması və məlumatları toplaması, çıxarması, dəyişdirməsi, şifrələməsi və ya məhv etməsi mümkündür. Həmçinin, pozulmuş kompüter sistemi tərəfindən idarə olunan prosesləri məhv etmək, dəyişdirmək və ya başqa şəkildə manipulyasiya etmək mümkündür.

Ümumiyyətlə, hər hansı bir davranış müəyyən bir aqressiv hərəkət həddinə çatdıqda və ya hərəkətin bu cür nəticələrə səbəb olacağına dair obyektiv ehtimal olduqda, düşmənçilik əlamətinin mövcud olması qəbul edilir [3]. Tallin 2.0 Təlimatının hazırlanmasında iştirak edən bəzi (azlıq) ekspertlər hesab edirlər ki, komponentin dəyişdirilməsini deyil, məlumatların bərpasını tələb edən bir obyektin funksionallığının itirilməsinə səbəb olan kiberəməliyyat düşmənçilik hərəkəti təşkil edir. Bu mütəxəssislərə görə, funksionallığın itirilməsinin maddi və ya mənəvi mənşəyi əhəmiyyətsizdir, vacib olan zərəri təşkil edən sonuncudur [8].

"Düşmənçilik" anlayışına "hərbi əməliyyatlara və ya digər tərəfin hərbi potensialına istənilən səviyyədə birbaşa zərər vurmaqla silahlı münaqişədə bir tərəfi dəstəkləmək üçün xüsusi olaraq həyata keçirilən bütün zorakı və qeyri-zorakı fəaliyyətlər" daxildir. Başqa sözlə, düşmənçilik hərəkətlərinə düşmənin hərbi imkanlarına mane olan hərəkətlərlə yanaşı, zorakı nəticələrə səbəb olan hərəkətlər də daxildir. Məsələn, elektrik enerjisini və ya rabitəni kəsmək düşmənçiliyin bir hissəsidir. Digər tərəfdən, qarşı tərəfə dolayı yolla təsir edən hər hansı bir davranış müharibə səylərinin bir hissəsi olsa da, düşmənçilik təşkil etmir. Əsgərlərin təlimi, müharibə üçün maliyyə resurslarının səfərbər edilməsi və ya silah istehsalı da düşmənçilik təşkil etməyən hərəkətlər arasındadır. Ona görə də kiberəməliyyatlar hərbi hədəfi "neytrallaşdırmaq" təsiri göstərərsə, beynəlxalq humanitar hüququn tənzimləmə dairəsinə düşə bilər.

Tallin 2.0 Təlimatının 14-cü Qaydası kiberhücumun silahlı münaqişə ilə əlaqəliliyini aşağıdakı meyarlar əsasında müəyyənləşdirmişdir [7]:

- Qanunsuzluq. Dövlətlər beynəlxalq səviyyədə qanunsuz hərəkətlərinə görə məsuliyyət daşıyır [11]. Beynəlxalq səviyyədə qanunsuz hərəkət elə bir hərəkət və ya hərəkətsizlikdir ki, hər ikisi: (1) həmin dövlətə tətbiq edilən beynəlxalq hüquqi öhdəliyin pozulmasını təşkil edir; və (2) beynəlxalq hüquqa əsasən dövlətə aid edilir. Hər iki elementin olmaması dövlətin sözügedən hərəkətə görə məsuliyyətini istisna edir. Kiberməkanda beynəlxalq səviyyədə qanunsuz hərəkət ya sülh dövrünü tənzimləyən qaydaların, ya da silahlı münaqişədə tətbiq olunan qaydaların pozulmasından ibarət ola bilər. Məsələn, sülh dövründə sahil dövlətinə qarşı ərazi dənizində yerləşən gəmidən kiberəməliyyatlar aparan dövlət günahsız keçid rejimini pozur (Qayda 48). Əgər dövlət silahlı münaqişə zamanı mülki obyektlərə qarşı kiberhücumlar (Qayda 92 və 100) həyata keçirirsə, o, silahlı münaqişə qanununu (Qayda 99) pozur və beləliklə, beynəlxalq səviyyədə qanunsuz hərəkət törətmiş olur.

- Coğrafi məkandan asılı olmama. Ümumi məsələ olaraq, kiberəməliyyatın beynəlxalq səviyyədə qanunsuz xarakteri onun başladığı coğrafi yerdən asılı deyil. Məsul dövlət öz ərazisindən, zərər çəkmiş dövlətin ərazisindən, başqa bir dövlətin ərazisindən, açıq dənizlərdən, beynəlxalq hava məkanından və ya kosmosdan beynəlxalq hüquqi öhdəliyin pozulmasını təşkil edən kiberəməliyyatlar həyata keçirə bilər. Xəbərdarlıq edilməlidir ki, müəyyən beynəlxalq səviyyədə qanunsuz hərəkətlər, xüsusən də kosmos, hava məkanı və

dənizlə bağlı coğrafi cəhətdən asılıdır. Misal üçün, keçid rejiminin pozulması (Qayda 48) müvafiq gəminin əməliyyat zamanı sahil dövlətinin ərazi dənizində kiberəməliyyat aparmasını tələb edir. Beynəlxalq hüquqi öhdəliyin pozulmasına əlavə olaraq, kiberhücumlarla əlaqəli hərəkətlər bu Qaydanın əhatə dairəsinə düşmək üçün konkret dövlətə aid edilməlidir.

BMT Nizamnaməsinin 51-ci maddəsi heç bir konkret silaha istinad etmədiyi üçün bu maddə baxımdan, hücumun ənənəvi vasitələrlə və ya kiber vasitələrlə həyata keçirilməsində heç bir fərq yoxdur. Eyni zamanda, Tallin Təlimatının 13-cü Qaydasına görə, silahlı hücum səviyyəsinə yüksəlmiş kiber əməliyyatın hədəfi olan dövlət özünümüdafiə hüququndan istifadə edə bilər. Kiber əməliyyatın silahlı hücum təşkil edib-etməməsi onun miqyasından və təsirlərindən asılıdır [7, Qayda 13]. Bildiyimiz kimi, hər hansı əşyanın silah kimi qəbul olunması üçün əsas meyarlar istifadə məqsədi, təyinatı və yaratdığı təsirdir. Buna görə də insan həyatına və/və ya əmlakın məhv edilməsinə səbəb olan hər hansı bir cihazın istifadəsi silahlı hücum üçün kifayət qədər hesab edilməlidir. Praktikada əmlakın məhv edilməsinə və ya insan itkisinə səbəb olmadan əhəmiyyətli narahatlıq yaradan kiberhücum güc tətbiqi hesab edilə bilər, lakin silahlı hücum kimi təsnif edilmir. Yalnız bu təsirlərə nail olan kiberhücum silahlı hücum kimi təsnif edilə bilər və zərərçəkmiş dövlətin özünümüdafiə üçün güc tətbiqinə müraciət etmək hüququnu şərtləndirə bilər. Deməli, qəzaya səbəb olmaq məqsədi daşıyan hava nəqliyyatının idarəetmə sistemlərinə edilən kiberhücum silahlı hücum hesab ediləcək, çünki belə bir hücumun insan həyatının və əmlakının məhv edilməsi ilə nəticələnə biləcəyi proqnozlaşdırıla bilən nəticələr vardır.

Kiberhücumun nəticələri fiziki olmadığı halda, 51-ci maddənin mənasında silahlı hücum təşkil edib-etməməsi mübahisəlidir. Məsələn, maliyyə mərkəzlərini hədəf alan kiberhücum əmlaka və ya fərdlərə birbaşa fiziki zərər vurmayacaqdır. Hədəfə əsaslanan yanaşmanı dəstəkləyənlər üçün kiberhücum fiziki ziyana səbəb olub-olmamasından asılı olmayaraq, vacib infrastrukturu hədəf aldığı və onu sıradan çıxarmağa çalışdığı andan etibarən silahlı hücum kimi xarakterizə edilə bilər. Estoniyada baş verən kiberhücum praktikası bir daha təsdiq etdi ki, təcrübədə fiziki zərər müşahidə edilmədiyi halda kiberhücumun silahlı hücum kimi qiymətləndirilməsi mümkün olmur.

Silahlı hücum müşahidə edildikdən sonra güc tətbiq etmək istəyən dövlət iki şərti yerinə yetirməlidir: cavab tədbirləri zəruri və mütənasib olmalıdır; silahlı hücum ya davam edən, ya da qaçılmaz olmalıdır. Silahlı hücuma cavab olaraq kibermüdafiədə güc tətbiq edildikdə, qeyd olunan şərtlər müdaxilənin ənənəvi metodlarla həyata keçirilməsi ilə eyni şəkildə yerinə yetirilməlidir. Buna görə də güc tətbiqinə bərabər olan kiberəməliyyatlar yalnız zəruri və mütənasib olduqda qanuni sayılacaqdır. Ona görə də dövlət özünü firewall kimi passiv kibermüdafiə tədbirləri ilə müdafiə edə bilirsə və ya güc tətbiq etmək həddinin altında aktiv tədbirlər görə bilirsə, özünümüdafiədə güc tətbiqi əsaslandırılmır. Mütənasiblik prinsipi güc tətbiqinin əhatə dairəsini, müddətini və intensivliyini silahlı hücuma son qoymaq

üçün zəruri olanla məhdudlaşdırır. Bu, istifadə edilən gücün özünümüdafiə vəziyyətinə səbəb olan hərəkətlə eyni miqyasda və ya təbiətdə olması demək deyil.

Bəzən dövlətlərin özünümüdafiə hüquqlarını həyata keçirmək istədikdə kiber tədbirlər görməli olduqları düşünülə bilər, çünki bunlar potensial olaraq silahlı təcavüzə ənənəvi tədbirlərdən daha az zərərlə son qoya bilər. Məsələn, fərdi olaraq silahlı hücum təşkil etməyən çoxsaylı paylanmış xidmətdən imtina hücumlarından ibarət kiber kampaniya kollektiv olaraq silahlı hücum kimi xarakterizə edilə bilər. Zərər çəkmiş dövlət məsul dövlətə qarşı tək bir kiberhücum etməklə cavab verə bilər. Özünümüdafiə əməliyyatı, həmçinin silahlı hücumun təsirlərinin artıq yarandığını və ya yaranma prosesində olduğunu nəzərdə tutur. Ona görə də kiberhücum artıq silahlı hücuma bərabər təsirlər yaratdıqda və ya bu cür təsirlər hazırda tətbiq edildikdə güc tətbiqi qanunidir.

IV. Nəticə

Beləliklə, Beynəlxalq Qızıl Xaç Komitəsi üçün beynəlxalq humanitar hüququn silahlı münaqişə zamanı kiberəməliyyatlara tətbiq edilməsi və buna görə də onları məhdudlaşdırması şübhəsizdir. Bu mövqe adıçəkilən sənəddə iki aspektdən əsaslandırılır. Birincisi, silahlı münaqişədə yeni və ya köhnə olsun, istənilən digər silah, vasitə və müharibə metodlarının istifadəsi beynəlxalq humanitar hüququn tənzimetmə dairəsinə düşdüyü üçün kiberməkanın hava, quru, dəniz və kosmosa bənzər yeni bir müharibə sahəsi kimi qəbul edilməsindən asılı olmayaraq, əhəmiyyətli zərər vuran kiberəməliyyatlar silahlı münaqişə ilə bərabər tənzimlənməlidir. İkincisi, Komitə kiberəməliyyatları üsul və vasitə kimi qiymətləndirildiyi üçün Beynəlxalq Ədalət Məhkəməsinin Nüvə silahları ilə təhdid və ya istifadənin qanuniliyi haqqında Məsləhət Rəyinə istinad edir: Silahlı münaqişədə tətbiq olunan beynəlxalq humanitar hüququn müəyyən edilmiş prinsipləri və qaydaları gələcəyin silahları da daxil olmaqla, bütün müharibə formalarına və bütün növ silahlara tətbiq olunur və bu, silahlı münaqişə zamanı kiberəməliyyatların istifadəsinə də aiddir.

ƏDƏBİYYAT (REFERENCES):

1. 10 Steps to Cyber Security: URL:https://www.ncsc.gov.uk/files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf (last access: 15.07.2025).
2. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. URL: https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949 (last access: 15.07.2025).
3. ICRC position paper. International Humanitarian Law and Cyber Operations during Armed Conflicts. URL: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (last access: 15.07.2025).

4. Internet activism. URL: https://www.ebsco.com/research-starters/social-sciences-and-humanities/internet-activism (last access: 15.07.2025).
5. Kaspersky. What is Cybersecurity? Definition, Types, and Tips. URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (last access: 15.07.2025).
6. National Cybersecurity Center of the Republic of Azerbaijan (in Azerbaijani / *Azərbaycan Respublikasının Milli Kibertəhlükəsizlik Mərkəzi*). URL: https://ncsc.gov.az/main-page (last access: 15.07.2025).
7. Tallinn Manual 2.0 On the international law applicable to cyber operations. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. URL:https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf (last access: 15.07.2025).
8. Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't. URL: https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ (last access: 15.07.2025).
9. The Australian Cyber Security Centre (ACSC). URL: https://www.cyber.gov.au/ (last access: 15.07.2025).
10. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://www.nist.gov/cyberframework (last access: 15.07.2025).
11. UN GGE. Articles on State Responsibility. URL:https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (last access: 15.07.2025).

Assessment of cyberattacks as armed conflict: a study based on international law

MEHDI ABDULLAYEV*

Abstract

The article examines the qualification of cyberattacks as armed conflicts under international legal norms (the UN Charter, the Geneva Conventions and their Additional Protocols, the Tallinn Manuals, and others). As is known, the main goal of international legal regulation is to ensure international peace and security, as stipulated in the UN Charter. The digitalization of modern society and the lack of clarity of the boundaries of cyberspace raise completely new issues

* Doctor of Legal Sciences, Academy of Public Administration under the President of the Republic of Azerbaijan / email: mehdi.k.abdullayev@gmail.com

in the implementation of this goal. Thus, any cyberattack committed in cyberspace can cause various economic, political and other damages not only to one state, but even to several states at the same time. Today, "paralyzing" the activities of any state with a cyberattack aimed at the critical information infrastructure of that state has become a very easy and easily controlled illegal activity. At present, these threats are further increasing. The main goal of the presented article is to propose a solution to the difficulties faced by international law during cyberattacks. For this purpose, the concept and main characteristics of cyberattacks and cyberattackers were examined, and the possibility of assessing a cyberattack as an armed conflict based on international documents was studied. At the same time, a comparative analysis is undertaken of the provisions of a number of important international instruments and the positions of international organizations (hard law and soft law norms). At the end of the study, it was concluded that cyberattacks themselves are hostile behavior, and it was argued that they are as dangerous as armed conflicts and that states have the right to self-defense against such attacks.

Keywords: *cyberspace, cyberattack, armed conflict, armed attack, the right of self-defence, cyberoperation, cyberespionage, cyberactivism, UN Charter, Tallinn Manual.*

Квалификация кибератак как вооружённого конфликта: исследование на основе норм международного права

МЕХДИ АБДУЛЛАЕВ*

Резюме

В статье на основе норм международного права (Устав ООН, Женевские конвенции о защите жертв войны и Дополнительные протоколы к ним, Таллиннское руководство и др.) анализируется вопрос квалификации кибератак как вооружённого конфликта. Как известно, основной целью международно-правового регулирования, как это предусмотрено Уставом ООН, является обеспечение международного мира и безопасности. Цифровизация современного общества и отсутствие чётких границ киберпространства выдвигают принципиально новые проблемы в реализации этой цели. Так, посредством любой кибератаки, совершённой в киберпространстве, возможно причинение различного экономического, политического и иного ущерба не только одному государству, но и одновременно нескольким государствам. На сегодняшний

* Доктор юридических наук, Академия государственного управления при Президенте Азербайджанской Республики / email: mehdi.k.abdullayev@gmail.com

день кибератака, направленная на критическую информационную инфраструктуру какого-либо государства, с целью «парализации» его деятельности, превратилась в легко осуществляемую и удобно управляемую противоправную деятельность. В настоящее время данные угрозы продолжают возрастать. Основной целью представленной статьи является предложение путей решения проблем, с которыми сталкивается международное право в условиях кибератак. С этой целью исследованы понятие и основные характеристики кибератак и киберпреступников, а также на основе международных документов изучена возможность квалификации кибератаки как вооружённого конфликта. Одновременно в сравнительном порядке проанализированы положения ряда важных международных документов и мнения международных организаций (нормы «жёсткого» и «мягкого» права). В заключение исследования сделан вывод о том, что сами кибератаки представляют собой поведение, носящее враждебный характер, в связи с чем они столь же опасны, как и вооружённые конфликты, а государства обладают правом на самооборону от подобных атак.

Ключевые слова: *киберпространство, кибератака, вооружённый конфликт, вооружённое нападение, право на самооборону, кибероперация, кибершпионаж, киберактивизм, Устав ООН, Таллиннское руководство.*

Redaksiyaya daxil olma tarixi: 25.07.2025
Çapa qəbul: 25.12.2025