https://doi.org/10.36719/2706-6185/44/98-101

Aysel Hacıyeva
Bakı Dövlət Universiteti
dissertant
hassanly.aysel@mail.ru

İnformasiya müharibəsinin hüquqi tərəfləri

Xülasə

Müharibə şəraitində qarşı tərəfə daha güclü zərbələr endirmək üçün müxtəlif təsir mexanizmləri mövcuddur. Daha güclü dövlətlərin hərbi doktrinalarında son dövrlərdə bu vasitələrdən biri də informasiya təsirləridir. Müharibə tərəflərinin istər müharibə şəraitində, istərsə də dinc dövrdə üstünlük əldə etmək məqsədilə bir birlərinin informasiya platformalarına hücum etməsi yeni müharibə üsulunun formalaşması ilə nəticələnmişdir.

İnformasiya müharibəsi müvafiq informasiya əməliyyatıdır ki, bu əməliyyat zamanı düşmənin obyekti informasiya, sənədləşdirilmiş informasiya, konfidensial informasiya, informasiya prosesləri, informasiya texnologiyaları, informasiya ehtiyatları və onların təminat vasitələri olur. Qarşı tərəf informasiya sistemlərinin kənar hücumlardan müdafiəsini təmin etməyə, eyni zamanda qarşı tərəf üzərində informasiya üstünlüyü əldə etməyə çalışır.

Açar sözlər: *informasiya, informasiya müharibəsi, Tallin təlimatı, informasiya texnologiyaları, informasiya sistemləri*

Aysel Hajiyeva
Baku State University
PhD student
hassanly.aysel@mail.ru

Legal Aspects of Information Warfare

Abstract

There are various mechanisms of influence to inflict stronger blows on the other side in wartime. In the military doctrines of more powerful states, one of these tools in recent times is information influence. The fact that the warring parties attack each other's information platforms in order to gain an advantage both in wartime and in peacetime has resulted in the formation of a new method of warfare.

Information warfare is a relevant information operation, during which the enemy's object is information, documented information, confidential information, information processes, information technologies, information resources and their means of support. The other side tries to ensure the protection of information systems from external attacks, and at the same time to gain information superiority over the other side.

Keywords: *information, information warfare, Tallin manual, information technology, information systems*

Giriş

"Haker hücumu" kimi tanın informasiya müharibəsi hücumunu necə xarakterizə etmək məsələsi, hələ tam inkişaf etdirilməyib.

İnformasiya müharibəsi zamanı qarşı tərəfə məxsus informasiya proseslərinə zərər yetirmək fəaliyyəti həyata keçirilir. Bu müharibədə hədəf olaraq düşmənin informasiyaların əldə olunması və nəticədə düşmənin iqtisadi və müdafiə sistemlərinə zərbələrin vurulmasıdır. Burada üç aspektdən məsələyə yanaşılır.

Birincisi ondan ibarətdir ki, qarşı tərəflər bir birinin informasiya vasitələrindən istifadə edərək dövlətin daxili və xarici siyasətinə müxtəlif vasitələrlə zərbələr yetirir.

İkincisi ondan ibarətdir ki, qarşı tərəflər bir birinin informasiya texnologiyalarını və sistemlərini fiziki mənada məhv etməyə çalışırlar. Burada ən önəmli faktorlardan biri düşmənə öz qüvvəsindən istifadə etmək imkanı verməməkdir. Belə ki, informasiya müharibəsinin əsas cəhətlərindən biri odan ibarətdir ki, silahdan istifadə etmədən düşmənin hətta silahdan istifadə etmək şansını sıfıra endirmək, həyati əhəmiyyətli maliyyə, bank, rabitə, elektrik və nəqliyyat vasitələrini məhv etmək mümkündür (Ələkbərova, 2012). Gündüyü kimi ən az klassik silahlar qədər dağıdıcı olan informasiya müharibəsi qarşı tərəfin döyüşən strukturlarını da sıradan çıxarmaq məqsədi daşıyır.

Üçüncüsü isə qarşı tərəfin əldə etməyə və ya məhv etməyə çalışdığı informasiyanı qorumaqdan ibarətdir.

Hər üç cəhd və bu cəhdə nail olmaq üzrə mübarizə müasir dövrdə informasiya müharibəsi adlanır. İnformasiya müharibəsinin bu formada aktual xarakter alması məhz informasiyanın cəmiyyətin bütün sferalarındakı rolunun nə dərəcədə üstün olması ilə bağlıdır. İnformasiya özünün ilkin və ana mənasından çıxaraq əlavə "yük" daşımağa başlamışdır. Belə ki, informasiya özünün məlumat təmin etmə funksiyasında əlavə müasir növ müharibənin predmeti və eləcə də obyekti olaraq iştirak edir.

Tədqiqat

İnformasiya müharibəsi hazırda dövlətlərin xarici siyasətlərində əsas silahlardan və metodlardan birinə çevrilmişdir. Lakin bu yeni müharibə növünə dair hələ də vahid bir fikir mövcud deyildir. Bununla belə hadisəyə dair hələ ki, ümumi bir fikir formalaşmasa da, dünya siyasətində meydana gələn yeni tendensiyalar onu göstərir ki, yeni norma və prinsiplərin əsasını qoymağın vaxtı çatmışdır.

Belə ki, informasiya müharibəsini tənzimləyən hüquqi normaları ehtiva edən, eləcə də informasiya silahından istifadəyə qadağa və məhdudiyyətlər müəyyənləşdirən normalar haqqında müvafiq konvensiyanın hazırlanması zərurəti özünü daha qabarıq göstərir (Nilz, 2011).

Amerika Birləşmiş Ştatları müvafiq sahədə dərin inkişaf yolu keçmişdir və tədqiqatlar aparmışdır. Bugün Amerika Birləşmiş Ştatları informasiya müharibəsinin həyata keçirilməsində digər ölkələrlə müqayisədə əhəmiyyətli dərəcədə üstündür. Əvvəllər informasiya mübarizəsi döyüş zamanı müəyyən tapşırıqların həyata keçirilməsi məqsədilə istifadə edilirdisə, hazırda isə birbaşa olaraq müharibənin əsas hərəkətverici qüvvəsi və həyata keçirilmə özülüdür. Müvafiq məsələyə dair ilk rəsmi material Pentaqonun "İnformasiya müharibəsi" adlı 21 dekabr 1992-ci il tarixli direktivi qəbul edilə bilər (Andrzej, 2014).

1993-cü ildə Baş qərargah Rəisləri Komitəsinin 30 saylı direktivində informasiya müharibəsinin ararılmasının əsas prinsipləri qeyd edilirdi. 1998-ci ilin sonlarında Amerika Birləşmiş Ştatlarının Baş Qərargah Rəisləri "İnformasiya əməliyyatlarının aparılmasına dair birgə doktrina" sənədini nəşr etdirdilər. Bu sənəddə Amerika tərəfindən informasiya əməliyyatlarının keçirilməsinin yalnız müharibə dövründə deyil, sülh dövründə də həyata keçirilməsi ilk dəfə olaraq adı çəkilən sənəddə ehtiva edilmişdir (Andrzej, 2014).

Amerika müvafiq sferada aparılan işlərin ancaq müdafiə xarakterli olduğunu iddia edirdi. Eyni zamanda müvafiq sferanın beynəlxalq norma və müqavilələrə uyğun olaraq tənzimləndiyini bəyan edirdi. Ancaq bu sahəyə aid beynəlxalq müqavilələr mövcud deyil.

"İnformasiya müharibəsi" termini ilk dəfə Amerika Birləşmiş Ştatlarının Müdafiə Nazirliyinin informasiya müharibəsi haqqında materiallarında bu formada qeyd olunur ki, informasiya həm silah, həm də məqsəddir: "İnformasiya hücumu isə icazə olmadan istənilən formada informasiyanın köçürülməsi, dəyişdirilməsi və məhvinə, habelə proqram təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatdır" (Georgetown University Law Library, 2024).

İnformasiya müharıəbsi ilə kibermüharibə çox əlaqəli olsalar da, bu anlayışların məzmunu bir birindən fərqlidir. Belə ki, informasiya müharibəsi kibermüharibəyə münasibətdə daha fenomendir və tarix boyu müharibənin tərkib hissəsi olmuşdur. Digər tərəfdən kibermüharibə nisbətən yeni bir hadisədir, belə ki, kibermüharibə çox əvvəl mövcud olan bir sıra informasiya müharibəsi əməliyyatlarından fərqli olaraq yalnız internetin və kompüterlərin icadından sonra ortaya çıxdı.

Kibermüharibəyə tətbiq edilən beynəlxalq hüquq üzrə Tallin Təlimatı (bundan sonra "Tallin Təlimatı") Estoniyanın Tallin şəhərində yerləşən Şimali Atlantika Müqaviləsi Təşkilatının (bundan sonra "NATO") Kooperativ Kiber Müdafiə Mükəmməllik Mərkəzinin təşəbbüsü ilə bir araya gətirilən bir qrup ekspert tərəfindən qəbul edilmiş iddialı layihə idi (Ahmad Qureshi, 2020, p. 901). O, 2009-cu ildə başlamış və üç ildən sonra Beynəlxalq Ekspertlər Qrupu (bundan sonra "Ekspertlər") kibermüharibəni tənzimləyən qanuna dair təlimat hazırlamışdır. Estoniya 2007-ci ildə bir çox ictimailəşdirilmiş kiberhücumların qurbanı olmuşdur ki, bu da kibermüharibənin təbiəti ilə bağlı, xüsusən də dövlətlər arasında davam edən hüquqi müzakirələrə təkan vermişdir (Kibermüharibəyə tətbiq edilən beynəlxalq hüquq üzrə Tallin Təlimatı, 2009).

Beynəlxalq hüququn kiberməkanda tətbiq edildiyi artıq mübahisəli deyildir. Birləşmiş Millətlər Təşkilatı (BMT) bildirmişdir ki, "beynəlxalq hüquq və xüsusilə Birləşmiş Millətlər Təşkilatının Nizamnaməsi müvafiq sahədə tətbiq edilir."

Dövlət Departamentin hüquq müşaviri Harold Koh 2012-ci ildə ABŞ-ın mövcud siyasətini ifadə etdi o, rəsmi olaraq bildirdi ki, beynəlxalq hüquq prinsipləri kiberməkanda tətbiq olunur. Daha da konkretləşdirsək qeyd edə bilərik ki, Tallin Təlimatının 80-ci Qaydasında beynəlxalq hüququn kibermüharibə üçün tətbiq olunduğu qeyd edilir (Johnson, 2010).

Beynəlxalq hüquq normalarının informasiya müharibəsinə tətbiq olunması dedikdə birbaşa müharibə qaydalarını tənzimləyən beynəlxalq humanitar hüququn normalarının tətbiqi nəzərdə tutulur. Müasir mənbələrə görə beynəlxalq humanitar hüququn normalarının informasiya müharibəsi zamanı tətbiq olunması birmənalıdır.

Nəticə

Məqalədə informasiya müharibəsi, onun səbəbləri, təhlükəllk dərəcəsi klassik müharibə ilə fərqləqləri araşdırılır. Kiber əməliyyatlar beynəlxalq humanitar hüquq məqsədləri üçün yalnız silahlı münaqişə kontekstində törədildikdə və fiziki zərər və ya zərərin nəzərəçarpacaq təhlükəsi mövcud olrasa və ya belə nəticəyə səbəb olarsa, "hücum" kimi qiymətləndiriləcək. Buna görə də bir çox kiber əməliyyatlar hücum kimi təsnif olunmasa da, beynəlxalq humanitar hüququn norma və prinsipləri bu münasibətlərə də kinetik silahlarla edilən hücumlara tətbiq olunduğu kimi tətbiq olunur. Mülki obyektlərə və ya mülki şəxslərə zərər vuran hərbi məqsədlərə qarşı yönəldilmiş kiber əməliyyatlar mütənasiblik testinə məruz qalır. Belə ki, mülki obyektlərə və ya mülki şəxslərə gözlənilən zərərin gözlənilən hərbi üstünlüklə müqayisədə həddən artıq olması ehtimalı varsa, bu akt hüquqazidd hesab olunacaqdır.

İnformsiya müharibəsi sahəsi ilə bağlı kinetik müharibəyə tətbiq olunan mövcud beynəlxalq hüquqi sənədlərin və diplomatik konvensiyaların şərhinə xeyli elmi səy sərf edilmişdir. Tallin Təlimatında və digər sənədlərdə mövcud humanitar qanunların kibermünaqişədə tətbiq oluna biləcəyi iddia edilir. Bura xüsusi qorunan statusun verilməsi konsepsiyası da daxildir. Kinetik müharibə mühitində qeyri-kombatantlar Qırmızı Xaç və Qızıl Aypara emblemləri və ya digər xüsusi işarələr kimi beynəlxalq simvollardan istifadə etməklə müəyyən edilə bilər. İnformasiya müharibəsi zamanı isə bir sıra yanaşmalara əsasən, sadə rəqəmsal markerlə sistemlərin müvafiq münaqişədə qorunan kimi müəyyən edilməsi təmin edə bilər (Peter, & Allan, 2014).

İnformasiya əməliyyatlarını tənzimləyən beynəlxalq hüququn nəzərdən keçirilməsi bir neçə nəticəyə gətirib çıxarır.

Birincisi, qanunun idarəedici orqanını faktiki olaraq müəyyən etmək vacibdir.

Üst-üstə düşən və kiberməkanda istənilən fəaliyyətə aid edilə bilən üç hüquqi rejim var-hüquq-mühafizə, kəşfiyyat məlumatlarının toplanması və hərbi əməliyyatlar.

İkincisi, informasiya əməliyyatının hərbi mahiyyətinin müəyyən edilməsi çox vacibdir. Belə ki, müdaxilənin sadəcə cinayət əməli yoxsa beynəlxalq hüquqa əsasən "güc tətbiqi" və ya "silahlı hücum" səviyyəsinə yüksəldiyini müəyyən etmək üçün prinsipial vasitə olaraq Şmitt təhlilinin yeddi amili (ciddilik, təcililik, birbaşalıq, invazivlik, ölçülə bilənlik, ehtimal olunan qanunilik və məsuliyyət) təklif edilir.

Üçüncüsü, əgər məlumat əməliyyatı kifayət qədər dağıdıcıdırsa, silahlı hücum hesab oluna bilər. Belə olan halda cavab tədbiri beynəlxalq hüququn silahlı münaqişələr zamanı dörd adət prinsipləri rəhbər tutulmalıdır - ayrı-seçkilik, zərurət, mütənasiblik və cəngavərlik. Bu prinsiplər kinetik

əməliyyatlar zamanı tətbiq olunduğu kimi bərabər şəkildə informasiya əməliyyatlarına da tətbiq olunur. Bu prinsiplər ümüharibə cinayətkarına çevrilmədən gücü müdafiə qurmaq istəyən kombatantlara aydınlıq ifadə edir.

Ədəbiyyat

1. Ahmad Qureshi, W. (2020). Information warfare, international law, and the changing battlefield. Fordham International Law Journal, 43, 901.
2. Andrzej, K. (2014). Comparative analysis of cyberattacks on Estonia, Georgia, and Kyrgyzstan. European Scientific Journal, 237, 242-243.
3. Ələkbərova, İ. Y. (2012). İnformasiya müharibəsi texnologiyaları. Ekspress-informasiya, "İnformasiya texnologiyaları" nəşriyyatı.
4. Georgetown University Law Library. (2024). The Tallinn Manual and primary law applicable to cyber conflicts. Retrieved from https://guides.ll.georgetown.edu/cyberspace/cyber-conflicts
5. Johnson, P. A. (2010). Is it time for a treaty on information warfare? In Computer network attack and international law.
6. Kibermüharibəyə tətbiq edilən beynəlxalq hüquq üzrə Tallin Təlimatı. (2009).
7. Nilz, M. (2011). Cyberwarfare and international law. UNIDIR Resources.
8. Peter, W. S., & Allan, F. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Daxil oldu: 21.10.2024
Baxışa göndərildi: 18.01.2025
Təsdiq edildi: 05.02.2025
Çap olundu: 28.02.2025