BAKI UNİVERSİTETİNİN XƏBƏRLƏRİ

№1 ***Sosial-siyasi elmlər seriyası*** ***2015***

UOT 343.21.7

KİBERTERRORİZMİN MAHİYYƏTİ HAQQINDA

E.B.EYYUBOVA
Bakı Dövlət Universiteti
elvira.eyyubova@gmail.com

Məqalədə kiberterrorizmin mahiyyəti haqqında fikirlər geniş təhlil edilir. Qloballaşan informasiya dövründə kibercinayət anlayışı o qədər geniş anlayışdır ki, onun cinayət tərkibi ilə bağlı müddəaları müasir informasiya texnologiyalarının inkişafına müvafiq olaraq və sürətli texnoloji tərəqqi nəzərə alınmaqla genişlənməsi ehtimalı böyükdür. Bu cəhətdən «kiberterrorizm» anlayışı bu kateqoriyaya aid edilə bilər. Belə qənaətə gəlinir ki, «kibercinayət» və «kiberterrorizm» anlayışları fərqləndirilməklə hər biri müstəqil cinayət tərkibi olaraq təsnif edilir və komyuterlər, kompyuter şəbəkələri, İnternet, sosial şəbəkələr yalnız «kiberterrorizm»in törədilməsində yardımçı vasitələr kimi qəbul edilir. Kompyuter sistemləri və ya şəbəkəsindən, o cümlədən İnternetdən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər etmişlərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hər hansı kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət əməlindən danışmaq mümkündür.

Açar sözlər: kiberterrorizm, kibercinayətlər, İnternet, Avropa İttifaqı, Avropol, kompüter hücumları, informasiya təhlükəsizliyi

Qloballaşan informasiya dövründə kibercinayət anlayışı o qədər geniş anlayışdır ki, onun cinayət tərkibi ilə bağlı müddəaları müasir informasiya texnologiyalarının inkişafına müvafiq olaraq və sürətli texnoloji tərəqqi nəzərə alınmaqla genişlənməsi ehtimalı böyükdür. Məsələn, «kiberterrorizm» anlayışı bu kateqoriyaya aid edilə bilər. Terror fəaliyyətində informasiya texnologiyalarından istifadə hal-hazırda özünün aktuallığı ilə müşayiət olunan ciddi bir problemdir və onun da əsas səbəbi informasiyanın energetika, nəqliyyat, telekommunikasiya obyektlərində, maliyyə idarələrində və bank sistemində həyata keçirilən fəaliyyətdə geniş tətbiq olunması ilə bağlıdır. Mahiyyəti üzrə terrorizmin bu yeni forması yüksək texnologiyanın cinayətkar məqsədlərlə istifadəsinin bir növüdür və buna görə də onu terrorçuluğun texnoloji növünə, o cümlədən kibercinayətlərin bir növünə aid etmək olar. Məsələ burasındadır ki,

müasir beynəlxalq hüquqda terrorçuluq ayrıca cinayət tərkibi kimi xüsusi statusa malikdir. Belə olan təqdirdə kiberməkandan terror məqsədləri ilə istifadə olunması, şəbəkə istifadəçilərinin də həm obyekti, həm də subyekti olduğu bu cinayət əməlinin terrorçuluq, yoxsa kibercinayətlərin xüsusi növü olması məsələsi bir qədər problemlərə yol açmış olacaqdır. Əlbəttə, bu kimi mübahisəli elementlərin aradan qaldırılması üçün bu sahədə unifikasiya olunmuş beynəlxalq cinayət hüquqi konsepsiyanın ortaya qoyulması və bu cinayət əməlləri ilə mübarizədə yeni tendensiyaların ortaya qoyulması zəruridir.

Bu məsələnin pozitiv həllində Avropa İttifaqı digər beynəlxalq strukturlardan daha fəal və operativ mövqe nümayiş etmişdir. Bu qurum tərəfindən İnternet şəbəkəsinin terror təşkilatları tərəfindən istifadəsi ilə mübarizə aparmaq məqsədilə Clean IT layihəsi işlənib hazırlanmışdır (4). Qeyd etmək lazımdır ki, bu cinayətlərlə mübarizədə xüsusi proqram və layihələrin hazırlanması üzrə Evropol-un xidmətləri danılmazdır. Həmin layihənin məqsədlərindən də göründüyü kimi, İnternet üzərindən həyata keçirilən qeyri-qanuni fəaliyyətlərə aid olan ictimai və özəl dialoq təşəbbüsləri xüsusi olaraq terrorçu fəaliyyətlərin fokuslanmasına gətirib çıxarır. Bu mənada onlayn terrorizmlə mübarizənin bilavasitə kibercinayətkarlıqla mübarizə ilə qarşılıqlı əlaqə və asılılıqda nəzərdən keçirilməsi fikrimizcə, faydalı olardı. Lakin, bu iki ayrı-ayrı cinayətlər öz tərkibləri etibarilə fərqləndiyindən, İnternet şəbəkəsi yalnız terror cinayətinin həyata keçirilməsinin vasitəsi olaraq qalacaqdır. Çünki, bu zaman terror cinayətinin törədilməsində əsas məqsəd kompyuter sistemləri və ya məlumatları deyil, terror cinayətinin qəsd obyekti olan ictimai təhlükəsizlik olacaqdır. Burada dövlətlərin səyi ondan ibarət olacaqdır ki, terrorçuluq cinayətinin qarşısının alınmasında yalnız məhdudlaşdırıcı informasiya texnologiya vasitələrinin köməyindən istifadə etməklə, onlayn terrorizmin fəsadları minimuma endirilsin.

Həmçinin bu məsələdə daha müfəssəl yanaşmanın ortaya qoyulması üçün «kiberterrorizm terminin» yaranma tarixinə də diqqətin ayrılması zəruridir. XX əsrin 80-ci illərinin sonlarında Amerika Təhlükəsizlik və Kəşfiyyat İnstitutunun (İnstitute for Security and İntelligence) böyük elmi işçisi Berri Kollin virtual fəzada terrorçuluq fəaliyyətini ifadə etmək üçün ilk dəfə «kibernetik terrorçuluq» terminindən istifadə etmişdir. Qeyd olunmalıdır ki, o zaman bu termin praktiki əhəmiyyət kəsb etmirdi və yalnız gələcək üçün proqnoz verməkdən ötrü istifadə olunurdu. Berri Kollinin özü isə kiberterrorçuluqdan yalnız XXI əsrin ilk onilliyində danışmağın real olduğunu qeyd etmişdir. Lakin real vəziyyətlə əlaqədar olaraq, FTB-nin xüsusi agenti Mark Pollit 1996-cı ildə kiberterrorçuluq termininin tərifini təklif etmişdir (1). Həmin tərifə görə, kiberterrorizm informasiya, kompyuter sistemləri, kompyuter proqramları əleyhinə yönələn, milli qruplara və mülki hədəflərə qarşı zorakılıqla nəticələnən siyasi motivli qəsdən törədilən hücumdur (7, p. 285-289).

Kiberməkanda terrorizm həm kibercinayət, həm də terrorizmin əlamətlərini özündə ehtiva edir. Kiberməkanda terror hücumları kiber cinayətin ka-

teqoriyası və informasiya texnologiyalarından kriminal sui-istifadə kimi çıxış edir (3).

Qeyd olunduğu kimi, kiberterrorçuluq və informasiya təhlükəsizliyi müasir dövrün real vəziyyətinə əsaslanaraq, hüquq və informatika mütəxəssislərinin məşğul olduğu ciddi bir problemə çevrilmişdir. Kiberterrorçuluqla bağlı hərəkət və hərəkətsizlik artıq real olaraq baş verməkdədir. Bu, həm digər cinayətlərin, xüsusilə terrorun və təcavüzün törədilməsi üçün hərəkətverici vasitə olaraq, həm də müstəqil cinayət tərkibi olaraq artıq dünya birliyi tərəfindən cəzalandırılmalı olan əməllər kateqoriyasına aid edilmişdir. Bununla yanaşı, bu günkü Azərbaycan reallığında kibermüharibənin, kibertəcavüzün və digər beynəlxalq cinayətlərin qurbanı kimi artıq bu əməllərə görə cinayət hüquqi yurisdiksiyanın həyata keçirilməsini labüd və zəruri etmişdir. Səmərəli cinayət hüquqi yurisdiksiyanın tətbiqi üçün isə kiberməkanda baş verən hərəkət və hərəkətsizlikləri özündə ehtiva edən hüquqi terminlərin istər nəzəri, istərsə də normativ hüquqi müəyyənliyə malik olması danılmazdır.

Ümumiyyətlə, kiberterrorçuluq dedikdə, kompyuterdə emal olunan informasiyaya, kompyuter sisteminə və şəbəkəsinə düşünülmüş, siyasi motivlərə əsaslanmış hücum başa düşülür. Əgər belə hərəkətlər ictimai təhlükəsizliyin pozulması, əhalinin qorxudulması, hərbi konfliktlərin, təxribatlarının törədilməsi məqsədilə həyata keçirilmiş olarsa, onda bu hücum insanların həyatı və sağlamlığı və ya digər ağır fəsadların baş verməsi üçün daha böyük təhlükə yaradır.

Kiberterrorizm siyasi, dini və ideoloji motivlər əsasında dağıdıcı, təxribatçı və qorxu aşılayan nəticələrə səbəb olan, terroristlər tərəfindən informasiya infrastrukturuna edilən hücumlar kimi müəyyən edilir (6, p.14). Təhlükəsizlik sahəsi üzrə bəzi ekspertlər hesab edirlər ki, kompyuter hücumu o halda kiberterrorizm kimi müəyyən edilə bilər ki, əgər belə hücumun nəticəsi kifayət qədər dağıdıcı olmuş və ənənəvi terror aktlarının nəticələrindən yaranmış nəticələrlə mütənasiblik təşkil edirsə (enerji təchizatında ciddi fasilələrin baş verməsi, təyyarənin qəzaya uğraması nəticəsində böyük insan tələfatı, ölkənin maliyyə-kredit sisteminə inamın itməsi və s.,) (5, p, 4-5; 9, s. 163-168). Kiberterrorçuluq cinayətkar niyyətlərin əldə olunması məqsədilə əhalinin, hakimiyyət orqanlarının qorxudulması kimi qəbul edilir. Bu, müəyyən siyasi və ya digər məqsədlərin əldə olunması, şəxslərin, təşkilatların və ya hakimiyyət strukturlarının müəyyən hərəkətlərə məcbur edilməsi, kiberterrorçunun şəxsiyyətinə və terrorçu təşkilata diqqətin yönəldilməsi məqsədilə əhalinin təhlükəyə məruz qoyulması, daimi qorxu vəziyyətində saxlanması şəklində özünü göstərə bilər. Transmilli mütəşəkkil cinayətkar qrupların müasir informasiya-kommunikasiya texnologiyalarından geniş miqyasda istifadə etməsi labüd faktdır. Beynəlxalq terrorçu təşkilatlar elmi-texniki nailiyyətlərdən yararlanmağa, kompyuter, rabitə, informasiya-kommunikasiya texnologiyaları və s. sahələrdə mütəxəssisləri öz sıralarına cəlb etməyə çalışırlar. Bu terrorçu təşkilatlar tərəfindən daim yeni üzvlərin rekrut edilməsi, törədilmiş terror aktlarına

bəraət qazandırılması, potensial terrorçulara təlimlərin keçirilməsi, üzvlər arasında müntəzəm əlaqələrin saxlanılması və s. məqsədlərlə İnternet şəbəkəsindən fəal istifadə edilir (2).

Bəzi ədəbiyyatlarda kibercinayətkarlığın bu növü elektron vandalizm də adlandırılır. Orada bu cinayət növü çox ciddi problem kimi səciyyələndirilərək, qeyd olunur ki, bu gün iqtisadiyyat, idarəetmə, hətta dünyanın əksər ölkələrinin ayrı-ayrı vətəndaşları kompyuter şəbəkə və sistemlərinin normal fəaliyyətindən asılıdır. Bu tipli cinayətlərin motivi ya öz iradəsini reallaşdırmaq, ya qisas və ya intiqam almaq istəyi, ya da rəqiblə hesablaşmaq istəyi ola bilər. Belə olan təqdirdə kompyuter sistemləri zədələnir və onların işinə olan müdaxilələr daha ciddi və bəzən də daha faciəvi nəticələrə səbəb ola bilər (8, s.11). Məsələn 1992-ci ildə kompyuter sisteminə edilən müdaxilənin nəticəsi idi ki, Litvada İqnalinsk Atom Elektrostansiyasında böyük bir nüvə partlayışlarına səbəb ola biləcək hadisələrin yaşanma ehtimalı yaranmışdı. Göründüyü kimi, kompyuterlərə edilən hətta təsadüfi müdaxilələr belə ağır fəsadları ilə xarakterizə olunan digər beynəlxalq cinayətlərin törədilməsinin əsas səbəbi kimi çıxış edə bilər. Bu səbəbdən də qeyd olunan cinayət növlərini kompyuter cinayətləri ilə əlaqəli cinayətlər kimi adlandırmaq fikrimizcə daha məqbul olardı. Lakin əsas məqsədini və hədəfini məhz kompyuter sistemləri və ya kompyuter şəbəkələri təşkil edən cinayətləri isə birbaşa kibercinayətlər kateqoriyasına aid etmək olar. Məsələn, 1999-cu ildə Belqradın bombalanması zamanı NATO-nun kompyuter sistemlərinin hədəflənməsi və onların işinin iflic olunması ilə bağlı həyata keçirilmiş cəhdlər kibercinayət kimi tövsif oluna bilər. Bu mənada kibercinayətlərdə əsas kriminal məqsədin məhz informasiya-kommunikasiya texnologiyalarına qarşı yönəldilməsi faktoru onun növlərə bölgüsündə əsas təsnifat meyarı kimi götürülməsi qəbul edilməlidir. Buradan da belə nəticəyə gəlmək mümkündür ki, əgər törədilən vandalizm və hər hansı istənilən dağıdıcı cinayətkar fəaliyyət məhz kompyuter sistemlərinin və şəbəkələrinin, habelə onlarda mövcud olan informasiyaların məhv edilməsinə yönəlmişdirsə, həmin əməlin törədilmə miqyasından və zahiri əlamətlərindən asılı olmayaraq, onları kibercinayətlər kateqoriyasına aid etmək olar. Digər tərəfdən, əgər kompyuter sistemləri və ya şəbəkəsindən, o cümlədən İnternet-dən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər etmişlərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hansısa kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət əməlindən gedəcəkdir.

Yuxarıda qeyd olunanları ümumiləşdirib belə bir nəticəyə gələ bilərik ki: 1) «kibercinayət» və «kiberterrorizm» anlayışları fərqləndirilməklə hər biri müstəqil cinayət tərkibi olaraq təsnif edilir və komyuterlər, kompyuter şəbəkələri, İnternet, sosial şəbəkələr yalnız «kiberterrorizm»in törədilməsində yardımçı vasitələr kimi qəbul edilir; 2) Kompyuter sistemləri və ya şəbəkəsindən, o cümlədən İnternet-dən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar

qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər etmişlərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hansısa kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət əməlindən danışmaq mümkündür.

ƏDƏBİYYAT

1. İnformasiya təhlükəsizliyi problemi və onu xarakterizə edən əsas amillər, http://referat.-ilkaddimlar. com/ref_info_5783
2. Mütəşəkkil cinayətkarlıqla mübarizə. http://www.mns.gov.az/az/pages/47-125.html
3. ARF Chairman's Statements and Reports , https://www.aseanregionalforum.asean.org/
4. Clean IT Project , https://www.edri.org/files/cleanIT_sept2012.pdf
5. CRS report 32114. Computer attack and Cyber Terrorism: Vulnerabilities and Polisy İssues for Congress. October 17 2003.
6. International Handbook on Critical Information Infrastructure Protection (CIIP) 2006 Vol. II, page 14.
7. Mark M. Pollitt. "A Cyberterrorism Fact or Fancy?", Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285-289
8. Тимошкина Ю.М. Компьютерные преступления. Москва 2010. S. 11.
9. Павлова Л.В. Применимость обычных норм международного гуманитарного права в рамках борьбы с актами международного терроризма //Материалы международной конференции «Международное гуманитарное право: новые вызовы, новые испытания» (6-7 сентября 2007 г., г. Минск) Минск; Издательство Министерства юстиции Республики Беларусь, 2008, с. 163-168

О СУЩНОСТИ КИБЕРТЕРРОРИЗМА

Э.Б.ЭЙЮБОВА

РЕЗЮМЕ

Одной из главных угроз международной безопасности стал терроризм, который поставил перед многими странами задачу организации адекватного противодействия. На международном уровне терроризм давно проявил себя как не признающего границ феномена всемирного характера. Особенно это характерно для его новых технологических или высокотехнологических форм. Глобализация информационных процессов обусловила появление новой формы терроризма – кибертерроризма, который можно отнести к, так называемым, технологическим видам терроризма. По нашему мнению, можно выделить два вида кибертерроризма: 1) непосредственное совершение террористических действий с помощью компьютеров и компьютерных сетей; 2) использование киберпространства террористическими группами в организационно-коммуникационных целях и с целью шантажа, а также для непосредственного совершения терактов.

Ключевые слова: кибертерроризм, киберпреступления, Интернет, Европейский Союз, Европол, компьютерные атаки, информационная безопасность

ON THE ESSENCE OF CYBERTERRORISM

E.B.EYYUBOVA

SUMMARY

One of the main threats to international security is terrorism that has set many countries the task of organizing adequate countermeasures. At the international level, terrorism has proved ıue self as a phenomenon of global character, which does not recognize borders. This is especially true for its new technology and high-tech forms. Globalization of information processes led to the emergence of a new form of terrorism – cyberterrorism. Cyberterrorism can be attributed to the so-called technological forms of terrorism. In our opinion there are two kinds of cyberterrorism: 1) direct commitment of terror acts using computers and computer networks; 2) the use of cyberspace by terrorist groups for the organizational and communication purposes and for the purpose of blackmail, as well as for direct commitment of terror acts.

Key words: cyber-terrorism, cybercrime, Internet, European Union, Europol, computer attack, information security