UOT 351/354

# YENİ QLOBAL TENDENSİYA: KİBERTERRORİZMİN TƏHDİDLƏRİNİN ARTMASI FONUNDA

**Zahid Oruc**
zahidoruc@gmail.com
*Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu*
DOI: 10.30546/9878.2024.1.10.100.

***Xülasə.*** Məqalədə kiberterrorizmin yaranması və inkişafı tarixinə qısa nəzər salınır, kiberterrorizm anlayışı müasir dövrdə geniş vüsət alan yeni qlobal təhlükə tendensiyası kimi təhlil edilir, onun elmi mahiyyəti və xüsusiyyətləri, həmçinin kibercinayətlərin statistikasında onun yeri və rolu nəzərdən keçirilir. Beynəlxalq kiberterrorizmin geniş yayıldığı hazırkı dövrdə kibermüdafiənin təşkili və həyata keçirilməsi ilə bağlı məsələlərə diqqət yetirilir. Kiberterrorizm və kiberhücumların törətdiyi fəsadlar, yaratdığı təhlükələr və onların aradan qaldırılması yolları beynəlxalq təcrübə əsasında araşdırılaraq təhlil edilir.

Sistemli yanaşma əsasında kiberterrorizm fenomeni beynəlxalq birliyin və milli dövlətin təhlükəsizliyinə təhdid yaradan və dünya miqyasında siyasi məqsədlərə çatmaq üçün ən təsirli vasitələrdən biri kimi əsaslandırılır. Kiberterrorizmin gələcəkdə ən təhlükəli silaha çevriləcəyi vurğulanır və ondan müdafiənin yolları araşdırılır.

Məqalədə müasir cəmiyyətdə kompüter terrorizminə qarşı mübarizənin aktual problemləri ilə bağlı tədqiqat mənbələri əsasında aktual istiqamətlər müəyyənləşdirilir. Dövlətlərarası əməkdaşlığın prioritet formalarına toxunulur, həmçinin kiberterrorizmə qarşı mübarizənin səmərəliliyinin artırılmasına yönəlmiş zəruri tədbirlər qeyd edilir.

**Açar sözlər:** kiberterrorizm, qlobal tendensiya, kibertəhlükəsizlik, kiberhücumlar, kibermüdafiə, kiberordu, kiberterrorist şəbəkə, antikiberterrorizm

## Giriş

Qlobal geosiyasi məkanda tarixboyu mövcud olan üç ənənəvi məkana XXI əsrdə yeni, dördüncü məkan da əlavə edilmişdir. Torpaq/quru, su/dəniz, hava/kosmos kimi mövcud olan, müxtəlif əməliyyatların aparıldığı real məkanlarla yanaşı, yeni bir virtual müstəvi kibermәkan, kiberfəza meydana çıxmışdır.

Son 10 ildə dünya dövlətləri öz hərbi, siyasi, geosiyasi, iqtisadi, informasiya və s. fəaliyyətlərini bu amili nəzərə almaqla həyata keçirməyə məcburdur və artıq hərbi-siyasi gücünü kibertəhlükəsizlik üzrə xüsusi bölmələr yaratmaqla artırmaqdadır. 2010-cu ildə ABŞ-da Kiber Komandanlığının yaradılması ilə formalaşan yeni dördüncü məkan – kiberfəza rəsmi olaraq tanındı.

2023-cü ilin ən mühüm qlobal təhdidləri sırasına dünyada mövcud olan "Rəqəmsal Qütbləşmə", "Texnopolyar dünya" reallıq olaraq daxil edilmişdir. Hazırda dövlətlər qlobal texnologiya şirkətlərinin yeni rəqabət forması ilə üzləşir. "Rəqəmsal/informasiya suverenliyi"– yeni rəqəmsal geosiyasət formalaşaraq milli suverenliyə meydan oxuyur. Ənənəvi məkanlarda sərhədlər və "qırmızı xətlər" mövcud olduğu halda, kibermәkanda sərhəd anlayışının olmaması vəziyyəti çətinləşdirən məqamlardandır. Faktiki olaraq, transsərhəd və transmilli məkanlar kibertəhdidlərin əsas meydanına çevrilmişdir.

Məlumdur ki, dünya birliyi kiberhücumlarla 1980-ci illərdən bəri üzləşir. Lakin bugün kiberhücumların miqyası, vurduğu ziyanın əhatəsi dövlət qurumlarından tutmuş, idarəetmə sistemlərinə, "ağıllı" adlanan bütün texnoloji ekosistemə, kritik infrastruktur sistemlərinə və s. qədər kəskin şəkildə genişlənməkdədir.

Süni intellekt texnologiyalarının görünməmiş inkişafı ilə kibertəhlükələrin cəmiyyətə və dövlətə yaratdığı təhdidlər hər gün, hətta hər saat artır.

Nə qədər sürətli inkişaf etsə də, texnoloji amil deyil, insan bugün də internet məkanında qarşılıqlı təsirlərin fundamental amili hesab edilir. İnsanlar, real-offline dünyada özlərinə xas olan bütün qarşılıqlı əlaqə formalarını, eləcə də cinayət əməllərini, hətta müharibələri də infosferaya daşıyırlar. Kibercinayətkarlıq ən ciddi sosial problem olaraq, insan hüquqlarına, demokratiyaya və qanunun aliliyinə, eləcə də beynəlxalq sülh və sabitliyə qarşı əhəmiyyətli təhlükəyə çevrilməklə, böyük ictimai-siyasi təsirlərə malikdir.

Müasir dünyada informasiya texnologiyalarının sürətli inkişafının təsiri altında sosial məkanın yeni virtual ölçüləri formalaşır. Kiberməkan dedikdə, dünyanın kompüter şəbəkələrində baş verən proseslər toplusunun vasitəçilik etdiyi, insanların məskunlaşması və fəaliyyəti üçün başqa bir mühitə çevrilmiş sosial qarşılıqlı əlaqələrin xüsusi sahəsini ifadə edən "virtual" ölçülər nəzərdə tutulur. İnternetdən əlavə, kiberməkana bir çox başqa kompüter şəbəkələri, məsələn, transmillilər daxildir ki, onların vasitəsilə maliyyə axınları, müxtəlif birjalarda ticarət və kredit kartı əməliyyatları haqqında məlumatlar ötürülür.

Kiberməkanda müxtəlif maşın və mexanizmlər üçün idarəetmə sistemləri işləyir, məsələn, generatorlar, liftlər, nasoslar, nəqliyyat və enerji sistemləri üçün idarəetmə panelləri, dronlar, döyüş robotları, müxtəlifdiapazonlu raketlər və. s. Qeyd edilənləri nəzərə alsaq, kiberməkanı ayrı-ayrı şəxslərin, korporasiyaların, dövlətlərin və onların birliklərinin, dövlətlərüstü strukturların və qurumların informasiya, iqtisadi, siyasi və hərbi fəaliyyətlərinin mühüm sahəsi hesab etmək olar. Müasir dünyada dövlət sərhədləri tanımayan kiberməkan siyasi, iqtisadi, informasiya və mədəni rəqabətin ən mühüm sahəsinə çevrilir [1, s.152; 153].

Hazırda fiziki şəxslərin, firmaların və korporasiyaların, siyasi partiyaların və digər siyasi aktorların, bütöv dövlətlərin və dövlətlərüstü qurumların internetdən, həmçinin xidmət və məlumat almaq üçün zəruri olan digər informasiya texnologiyaları (İT) şəbəkələrindən asılılığı durmadan artır. Dövlət qurumlarına və özəl şirkətlərə kiberhücumlar çoxalır. Qeyd etmək lazımdır ki, bir-biri ilə əlaqəli informasiya infrastrukturuna planlaşdırılmış, həyata keçirilən və məqsədyönlü kiberhücumlar ciddi nəticələrə səbəb ola bilər.

Zaman keçdikcə şəxsi məlumatların məxfiliyi cəmiyyətin bütün səviyyələrini əhatə edən strateji, milli məsələyə çevrilir. Məhz bu səbəbdən kibertəhlükəsizlik informasiya cəmiyyətinin inkişafına töhfə verən amillərdən hesab edilir. Kibertəhlükəsizliyin təmin edilməsi sosial sabitliyin və rifahın əsas şərtlərindəndir [2, s.56].

## Kiberterrorizm anlayışı, elmi səciyyəsi və xüsusiyyətləri

Qlobal informasiya cəmiyyətinə keçid kontekstində dövlətlər, cəmiyyətlər, müəssisələr və fərdlər kiberməkanda məlumatın həqiqiliyi və mənbəyi, e-poçtda şəxsi məlumatların təhlükəsiz istifadəsi, mühafizəsi, bütövlüyü və məxfiliyi ilə bağlı kritik problemlərlə üzləşirlər. Yeni kibertəhlükələrin daim ortaya çıxdığı və təkmilləşdiyi bir mühitdə ölkələrin bu qlobal təhlükəyə qarşı çevik və operativ kibertəhlükəsizlik strategiyasına malik olması vacibdir.

XXI əsrdə kibercinayətkarlığın inkişafı ilə paralel olaraq ondan müdafiə sistemləri də inkişaf edir. Bununla belə kiberhücumların sayı durmadan artır və təkmilləşir.

Təhlükəsiz kiberməkanın yaradılmasında əsas problemlərdən biri kiberterrorizmdir.

Kiberterrorun sürətlə genişlənməsinin əsas səbəbi onun terrorçular, eyni zamanda sürətli terror hücumları üçün iqtisadi və effektiv üsul olmasıdır.

İlk vaxtlar informasiyanın saxlanması və mübadiləsi üçün bir vasitə olan internet, 2000-ci illərdən informasiyanın yaradıldığı məkana çevrildi. Qısa bir zamanda "dünya əhalisinin 5,16 milyarddan çoxu (64,4%) dünyanın rəqəmsal əhalisinə (worldwide digital population), yəni internet istifadəçisinə, 4,76 milyard əhali isə sosial şəbəkə istifadəçisinə çevrilmişdir ki, bu da hər il orta hesabla 200-250 milyon artım tempi deməkdir [3].

Bu qlobal transformasiya informasiya və kommunikasiya texnologiyalarına (İKT) artan tələbat və asılılıq sahəni hədəfə alanların və ya cinayətkarlıq məqsədilə ondan istifadə edənlərin çoxalması cəmiyyətlərə kibercinayətlər kimi yeni təhdidlər gətirdi. Son illər sürətlə inkişaf edən "süni intellekt"idə

öz cinayətkar əməlləri üçün istifadə edənlərin hədsiz çoxalması nəticəsində kibertəhlükələr qlobal xarakter aldı. Davosda ənənəvi keçirilən Dünya İqtisadi Forumun (The World Economic Forum) ekspertlərinin hazırladığı "Global Threats 2018" (Qlobal Təhdidlər 2018) hesabatında təbii fəlakətlərdən və qlobal istiləşmədən sonra kibercinayətlər sivilizasiyası bəşəriyyət üçün mühüm təhlükə olaraq qiymətləndirildi. Yeni cinayətkarlığın statistikası "qartopu effekti" ilə artmaqdadır. Belə ki, 2012-ci ildən başlayaraq 5 il ərzində dünyanın ən böyük şirkətlərinin kompüter sistemlərinin sındırılmasının sayı 2 dəfə artaraq, 68-dən 130-a çatmışdır [4].

Hər il, hətta hər ay yeni formaları ortaya çıxan kibercinayətlərin bitkin və əhatəli tərifi bugün üçün mövcud olsa da, natamam xarakter daşıyır. Bununla yanaşı, kibertəhdid və cinayətlərin çoxsaylı, dar və geniş mənada izah və tərifləri mövcuddur.

İnternet/informasiya sistemlərinə qanunsuz daxilolma, müdaxilə, habelə digər formalarda informasiya təhlükəsizliyinin pozulmasına yönəldilən səylər də kibertəhdid kimi səciyyələndirilir. Kibercinayətkarlıq maddi qazancdan başqa, (məs., dövlətin informasiya, yaxud digər kritik infrastrukturuna, strateji əhəmiyyətli dövlət obyektlərinə ziyan vurmaq kimi və s.) siyasi məqsədlər daşıyarsa, kiberterrorizm yaranmasına səbəb olur.

"Kiberterrorizm" termini ilk dəfə 1980-ci ildə Kaliforniya Təhlükəsizlik və Kəşfiyyat İnstitutunun (Institute for Security and Intelligence) baş elmi işçisi Barri Kollin tərəfindən istifadə edilmişdir [5, s. 23; 26]. Həmin illərdə internetin sələfi – ABŞ Müdafiə Nazirliyinin Perspektiv Tədqiqat Layihələri İdarəsinin ARPANET şəbəkəsi bir dövlətin ərazisində bir neçə onlarla kompüteri birləşdirdi. Tədqiqatçı belə sistemlərə müdaxiləni 21-ci əsrin ilk onilliyindən tez baş verməyəcəyinə inansa da, zaman keçdikcə kiberşəbəkələrin imkanlarının terrorçular tərəfindən mənimsəniləcəyini proqnozlaşdırmışdı.

Bildiyimiz kimi, zaman proqnozları qabaqladı. Belə ki, 1990-cı illərdə ilk kiberhücum cəhdləri hüquq-mühafizə orqanları tərəfindən artıq qeydə alınmışdı. Məsələn, 1993-cü ildə Litvada terrorçular "Troya atı" tipli zərərli proqram vasitəsilə kompüter nəzarətini ələ keçirərək "İqnalina atom elektrik stansiyasını" partlatmaqla hədələdilər. 1998-ci ilin iyununda "Milworm beynəlxalq haker qrupu" Hindistanın atom tədqiqatlarına giriş əldə etdi, "Bhabha Atom Tədqiqatları Mərkəzi (BARC)" adlı, təhlükəli saxta internet səhifəsi yaratdı. 1997-ci ildə Federal Təhqiqatlar Bürosunun xüsusi agenti Mark Pollit yeni bir hüquqi termini təqdim etdi və kiberterrorizmi "hərbi olmayan hədəflərə, əhaliyə və ya gizli agentlərə qarşı zorakılıqla nəticələnən informasiyaya, kompüter sistemlərinə, proqramlara və məlumatlara qəsdən, siyasi motivli hücum" adlandırdı [6].

Getdikcə yayılan, daha da mürəkkəbləşən kiberterrorizm bugün bəşəriyyət üçün ən böyük problemlərdən biri kimi dəyərləndirlir.

Kiberterorizmin spesifik xüsusiyyətlərinə aid edilir:

– kiberterrorizm kompüter və elektron şəbəkələrindən, müasir informasiya texnologiyalarından istifadə edilərək törədilən yeni terror formasıdır;

– aşağısəviyyəli aşkarlanma və yüksəkdərəcəli gizlilik səviyyəsinə malikdir;

– informasiya texnologiyalarının, kompüter sistemlərinin və xüsusi proqram təminatının istifadə edildiyi informasiya silahıdır;

– beynəlxalq aspektdə genişməqsədli əməliyyatlarla bağlıdır.

Yuxarıda qeyd edilənlərlə yanaşı, kiberterorizmin konkret ölkəni hədəfə almaq, cinayətkar və qurbanların ayrı-ayrı ölkələrdə olması kimi xüsusiyyətləri də vardır.

Qlobal miqyas və hədəfli kiberterrorizm əməliyyatlarında kiberhücumlar məhdud texniki dəstəkdən, aşağı maliyyə xərclərindən istifadə etməklə böyük maddi ziyana səbəb ola bilər. Kiberterrorizm araşdırmaçılar tərəfindən ictimai təhlükəsizliyi pozan, əhalini qorxutmaq məqsədilə törədilən, insanların həyatı və sağlamlığı üçün təhlükə yaradan, eləcə də hərbi münaqişəyə və ya digər ağır nəticələrə səbəb olan kompüter, kompüter sisteminə və ya şəbəkə tərəfindən işlənmiş məlumatlara hücum kimi izah edilir [7].

Kiberterrorizm yeni silahdır və dünya ictimaiyyəti üçün böyük təhlükə yarada bilər. Bu mərhələdə "etibarlı qorunma" adlandırılan sistemlər çox azdır. Enerji və nəqliyyat sistemini dəstəkləyən yüksək texnologiyalara sürətli çıxışı olan ölkələr üçün kiberterrorizm ciddi təhlükə yaradır. Bu, ümumilikdə

bəşəriyyət üçün ciddi təhlükədir. Demək olar ki, belə bir fenomenin tam öyrənilməyib, lakin onun nəticələrini təsəvvür etmək mümkündür. Göründüyü kimi, kiberterror hücumunun dəqiq sərhədləri mövcud deyil, o, konkret bir dövlətə, bəlkə də bütövlükdə bütün dünyaya yönəldilə bilər. Kiberterrorçunun aşkarlanması isə mürəkkəb bir prosesdir, çünki o, dünyanın istənilən ölkəsində yerləşə bilər. Virtual orijinallıq kiberterrorçuya diqqətdən kənarda qalmağa imkan verir. Və bu amillər ağır nəticələrə gətirib çıxara, eyni zamanda vətəndaşlar üçün təhlükə yarada bilər. Kiberterrorçuların silahı kompüter və internet, xüsusi proqram təminatıdır. Elektron şəbəkələr kiberterrorçulara dövlət sirri kimi təsnif edilən kompüter sistemlərinə icazəsiz daxil olmağa imkan verir. Kiberhücumlar vasitəsilə elektrik şəbəkələrini, aparat qurğularını məhv etmək, xüsusi proqramlardan tətbiqilə kiberməkanın ayrı-ayrı elementlərini zədələmək, strateji əhəmiyyət kəsb edən resursları oğurlamaq və pozmaq, virusları yaymaq, məxfi məlumatları açıqlamaq və yaymaq, həmçinin telekommunikasiya yayım kanallarını ələ keçirmək mümkündür (o cümlədən dezinformasiya, rabitə qovşaqlarının süni şəkildə yüklənməsi, rabitə xətlərinin məhv edilməsi məqsədilə də kibür hücumlar heyata keçirilə bilər).

Kiberterrorçuluğu digər kibercinayət növlərindən fərqləndirən əsas cəhət odur ki, onun hədəfi hazırda yüksək texnologiyalar, peyk rabitəsi və qlobal şəbəkələr sahəsində lider olan ölkələrdir. İstənilən ölkənin əsas infrastruktur elementlərinə kiberterror hücumunun edilməsi mümkündür. Kiberterrorun nəticələrinə aid edilir:

1. Simsiz modemlər və ya internet bağlantıları vasitəsilə idarəetmə sistemlərinə edilən hücum yerli elektrik enerjisinin müvəqqəti kəsilməsinə səbəb ola bilər.
2. Nəqliyyat-logistika sferasında kibertəcavüzkarın idarəetmə sistemlərinə qoşulmaq imkanı.
3. Dövlətin milli su ehtiyatlarına müdaxilə: internet vasitəsilə idarəetmə sisteminə hücum edərək, tərkibində xlor və digər kimyəvi maddələrin miqdarını artırmaq.
4. Enerji sferasında: kritik enerji infrastrukturunda enerji mənbələrinin müvəqqəti dayandırılması.
5. Maliyyə sahəsində: şəbəkə virusları vasitəsilə serverləri söndürmək və maliyyə bazarını çökdürmək.
6. İnformasiya texnologiyaları sahəsində: mövcud informasiya infrastrukturunun digər elementlərinə müxtəlif hücumların edilməsi, həmçinin "Ümumdünya Hörümçək Şəbəkəsi"ndə genişləndirilmiş kommunikasiya problemləri yarada bilən proqram təminatının zəif olması kritik sistemlərə çıxışı əlçatan edir [8, s. 44].

Kiberterorizmlə bağlı müxtəlif yanaşmalar mövcuddur. Belə ki, bəzi alimlər kiberterrorizmi internet beynəlxalq şəbəkəsinin, digərləri isə kompüter və telekommunikasiya texnologiyalarının istifadəsi ilə törədilən cinayət kimi qiymətləndirir [9, s.352].

Nisbətən yığcam ifadə edilən digər təriflərə görə kiberterrorizm istənilən müasir informasiya və taktikadan istifadə etməklə həyata keçirilir və onun fəaliyyət metodları siyasi terrorizmdən fərqlənir. İnformasiya terrorizmi, siyasi terrorizm üçün xarakterik olan məqsədləri ilə kiberməkana təsirin bu formalarından fərqlənir. İnformasiya-terror aktlarının həyata keçirilmə vasitələri müxtəlif ola bilər və müasir informasiya silahlarının bütün növlərini əhatə edir. Eyni zamanda onun tətbiqi taktikası və üsulları informasiya müharibəsi taktikası və informasiya cinayətinin üsullarından xeyli fərqlənir [10].

Kiberterrorizmi informasiya texnologiyalarından terror məqsədləri üçün istifadəni, ciddi iqtisadi nəticələrə səbəb olan yalançı kiberterror aktı təhlükəsini, kommunikasiya xətlərinin məhv edilməsini və ya aktiv şəkildə qarşısının alınmasını, yanlış ünvanın dəyişdirilməsini, keçid qovşaqlarının süni şəkildə yüklənməsini nəzərdə tutan onlayn cinayət əməli kimi izah edən tədqiqatçılar da vardır[11, s.178].

Bəzilərinin fikrincə, kiberterrorizmin mahiyyəti informasiya sistemlərinə qeyri-qanuni təsir göstərmək, texnogen xarakterli qəza və fəlakətlər, yaxud elə bir miqyaslı təhlükənin reallaşdırmaqdan ibarətdir ki, bu halda çox sayda şəxsin həyatına, sağlamlığına və ya əmlakına zərər vurmaq təhlükəsi meydana çıxır [12, s.66].

## Kibercinayətlərin statistikasında kiberterrorizm halları getdikcə artmaqdadır

2021-ci ilin oktyabrında qərargahı İsraildə yerləşən qlobal "Check Point" şirkəti bildirmişdi ki, dünyada kiberhücumların və kiberterror hadisələrinin sayı bir il ərzində 40% artıb. Əlavə olaraq, 2020-

ci illə müqayisədə korporativ şəbəkələrə hücumların sayında artım müşahidə olunur. Qeyd etmək lazımdır ki, bu hücumlara daha çox məruz qalanlar təhsil və tədqiqat saytları, dövlət və hərbi strukturlar, eləcə də rabitə sənayesindəki saytlardır .

Kibertəhlükəsizlik məsələləri uzun müddətdir ki, biznes üçün gündəlik təhdiddir. Məhsul və ya xidmətlə bağlı malların, məlumatların və maliyyə axınının idarə edilməsinə (istehsal üçün materialların harada və nə qədər alındığı, hazır məhsulun istehlakçıya necə çatması və s.) cavabdeh olan SCM sistemləri xeyli zəifləmişdir. Buna nümunə kimi 2021-ci ildə serverlər tərəfindən mal ətinin dəyərini artırmaqla hədələyən böyük Amerika ət emalı şirkətinin JBS-si sındırılmasını və nəticədə mal ətinin tədarük zəncirinin pozulmasını götərmək olar.

Daimi olaraq dəyişən xüsusiyyətləri ilə kibertəhlükəsizliyin 2023-cü il üçün maraqlı və narahatedici statistik xülasəsi belədir:

– 2022-ci ilin birinci yarısında 236,1 milyon kiberhücum baş vermişdir;
– 2022-ci ildə dünya üzrə təşkilatların 71%-i kiberhücumların qurbanı olmuşdur;
– kiberhücumları hər 10 saniyədə baş verir;
– bütün kiberhücumların 71%-i maliyyə motivlidir (ardınca əqli mülkiyyət oğurluğu, sonra isə casusluq gəlir);
– 2026-cı ilə qədər kibercinayətkarlıqdan illik qlobal zərərin 20 trilyon ABŞ dollarını keçəcəyi təxmin edilir;
– 2022-ci ildə kibertəhlükəsizlik sənayesi 156,3 milyard dollardan çox dəyərə malik olmuşdur;
– zərərli URL-lər 2021-ci ildən 2022-ci ilə qədər 61% artmışdır;
– kiberhücumların 76%-i etimadnamələrin toplanması ilə bağlı olmuşdur.

Cisco, Twilio və Uber kimi böyük təşkilatların yüksəkprofilli pozuntularının hamısı etimadnamə oğurluğu ilə bağlı idi;

Poneman İnstitutunun araşdırmasına əsasən, ABŞ xəstəxanalarına edilən kiberhücumlar ölüm nisbətini artırır, kiberhücumlar nəticəsində xəstələrin 59%-i xəstəxanada qalma müddətinin artırıldığını bildiriblər. Xəstəxanalara kiberhücumların təxminən 25%-i ölüm hallarının artması ilə nəticələnmişdir. ABŞ-ın səhiyyə sisteminə 12 kiberhücum nəticəsində 56 müxtəlif quruma zərər yetirilmişdir.

2020-ci ilin sentyabr ayında Almaniyanın Düsseldorf Universitet Xəstəxanasının işçiləri xəstələri təcili başqa yerə yönləndirməyə məcbur edən kiberhücuma məruz qalmışdır. Kiberhücum xəstəxananın bütün informasiya texnologiyaları (İT) şəbəkəsini məhv edərək, həkimlərin və tibb bacılarının bir-biri ilə əlaqə saxlamasına maneə yaratmış, həmçinin xəstələrin qeydlərinə daxil olmanı məhdudlaşdırmışdır[13].

## Kiberterrorizm və kibermüdafiə

Kiberterrorizmdən müdafiə mürəkkəb vəzifə olub, preventiv, kəşfiyyat yönümlüdür. Bu sahə fövqəladə hallara cəld reaksiyanı təmin edən CERT (Computer Emergency Response Team – Elektron təhlükəsizlik Xidməti) tipli təşkilati strukturların yaradılmasını tələb edir. Kibermüdafiə passiv və aktiv müdafiə formalarını əhatə edir. Aktiv müdafiə üsulları hücumçunun hücum xərclərini artıraraq, onun qarşısının alınması məqsədi daşıyır.

İkinci mühüm bacarıq, düşmən elementlərinin informasiya infrastrukturları üzərində strateji kiberəməliyyatlar həyata keçirməkdir. İkincisi ilə sıx bağlı olan üçüncü mühüm bacarıq, müharibə zamanı düşmənin İT infrastrukturlarına kiberhücumların təşkili ilə bağlıdır.

Dördüncü və sonuncu bacarıq informasiya texnologiyalarının təqdim etdiyi imkanlardan yararlanmaqla ənənəvi hərbi strukturları modernləşdirərək potensialın və səmərəliliyin artırılmasıdır.

İkinci sahə kibercinayətkarlıqla mübarizə məsələsidir. Mübarizənin birinci mərhələsi milli və beynəlxalq hüquqi infrastrukturun yaradılmasıdır. Bu tapşırıq, adətən, ədliyyə nazirlikləri vasitəsilə həyata keçirilir.

Ədliyyə nazirlikləri insan hüquq və azadlıqlarını haqsız yerə məhdudlaşdırmayan, çəkindirici təsir göstərən və polis bölmələri üçün mümkün qədər rahat iş şəraitini təmin edən hüquqi infrastrukturun yaradılması istiqamətində ölkə səviyyəsində iş aparmalıdır.

Kibercinayətkarlıq qlobal xarakter daşıdığından digər ölkələrin hüquq sistemlərinin inkişafına töhfə verməli və bu sahədə əməkdaşlıq mexanizmlərini inkişaf etdirməyə çalışmalıdır. Kibercinayətkarlıqla mübarizədə, bəlkə də ən mühüm vəzifə polis bölmələrinin üzərinə düşür. Polis bölmələrinin rəqəmsal araşdırma bacarıqlarını inkişaf etdirmək üçün ixtisaslaşmış mütəxəssislərə ehtiyac vardır. Transmilli cinayətlərin araşdırılması üçün xarici polis orqanları ilə ikitərəfli əlaqələrin qurulması bu sahədə lazım olan sürət və çevikliyi təmin edə bilər.

Kibercinayətkarlıqla mübarizənin digər ölçüsü kommersiya qurumları və qeyri-hökumət təşkilatlarıdır. Kibercinayətlər baxımından ən mühüm kommersiya qurumlarından biri də xidmət təminatçılarıdır. Ümumiyyətlə, bütün xidmət təminatçıları öz serverlərinə yönəldilmiş e-poçt trafikini filtrləyə bilərlər ki, istifadəçilər daha az spam e-poçtları alsınlar.

Eynilə, domen hostinqi (müəyyən icarə xidməti üçün internet səhifələrinin yerləşdirilməsi və nəşri) şirkətləri məzmunlarına edəcəkləri nəzarətlə kibercinayətkarlıqla mübarizə fəaliyyətlərində iştirak edə bilərlər. Qeyri-hökumət təşkilatları da istifadəçilərin informasiya sistemlərindən yararlanarkən daha şüurlu davranmalarına yardım edə bilərlər.

Üçüncü sahə olan kəşfiyyat, əks-kəşfiyyat fəaliyyəti ilk iki sahə ilə sıx bağlı olsa da, özünəməxsus xüsusiyyətlərə malikdir. Bugün kommersiya sirrini oğurlamaq məqsədilə təkcə dövlət qurumları arasında deyil, özəl şirkətlər arasında da kəşfiyyat işləri aparılır [14].

Hazırda kibermüdafiə ilə bağlı istedad böhranı mövcuddur və təşkilat rəhbərlərinin 30%-i təşkilatın kibertəhlükəsizliyini təmin edəcək kadrların olmadığını qeyd edir. Onlar bu problemi həll etmək üçün kibertəhlükəsizliyə təminat verəcək kadr hazırlığına ayrılan maliyyənin artırılmasını məqsədəuyğun hesab edirlər. Bir çoxları isə kibertəhlükəsizlik məqsədilə süni intellektdən istifadəyə üstünlük verir.

Milli kibertəhlükəsizliyin əsaslarından biri də kiberməkanda kəşfiyyat əməliyyatları aparmaq, habelə onlara qarşı mübarizə bacarıqlarını təkmilləşdirməkdir.

Dördüncü sahə kibertəhlükəsizlik böhranının idarə edilməsi və kritik infrastrukturların qorunmasıdır. Böhranlı vəziyyəti idarəetmə bacarıqlarına kiberhücumlara məruz qaldıqdan sonra zərərin aşkarlanması, hücumlara və fövqəladə hallara cavab verilməsi, zədələnmiş sistemlərin bərpası kimi kritik funksiyalar daxildir.

Qeyd etdiyimiz vəzifələr, adətən, milli CERT bölmələri tərəfindən yerinə yetirilir. CERT bölmələrinin yaranan təhlükələr üzrə təlim keçməsi və təhlükəsizlik bölmələri ilə əməkdaşlıq etməsi vacibdir.

Kritik infrastrukturların mühafizəsi, ilk növbədə milli risk təhlilini və risk faktorlarının mütəmadi olaraq yenilənməsini tələb edir. İkinci olaraq, kritik infrastrukturlar üçün standartlar hazırlanmalı, lazım gələrsə, qanunlar vasitəsilə özəl və ictimai əhəmiyyətli infrastrukturlar bu standartlara uyğunlaşdırılmalıdır.

Beşinci və son sahə kiberdiplomatiya və internetin idarə olunmasıdır. Kiberməkan yeni formalaşdığından, xüsusilə güclü dövlətlər daim bu yeni sahə ilə bağlı qaydaların öz milli maraqlarına uyğun olmasına çalışırlar. Bu səbəbdən milli maraqlara zidd hər hansı bir fəaliyyətin olmaması üçün kiberdiplomatiyaya önəm verilməlidir. Digər bir məsələ internetə rəhbərlik edən siyasət və standartlardır.

İnternet yarandığı gündən heç bir dövlətin və ya özəl qurumun birbaşa təsiri altında olmayıb. Mərkəzi strukturun olmaması hər cür fikirlərin sərbəst ifadə olunduğu mühitin yaradılmasına kömək edir, lakin internetin təhlükəsizliyinə mənfi təsir göstərir. İnterneti daha etibarlı etmək üçün şirkətlər və müstəqil təşkilatlar təhlükəsiz rabitə protokollarının və standart proseslərin inkişafı üzərində işləyirlər.

İnsan elementi təhlükəsizliklə bağlı bir çox sahədə olduğu kimi, kibertəhlükəsizlikdə də ən mühüm amildir. Sistemdə nə qədər təhlükəsizlik tədbirləri görülsə də, diqqətsiz istifadəçi tərəfindən məğlub olmaq riski həmişə mövcuddur.

Dimensional Research firmasının 2011-ci ildə sosial mühəndislik hücumları ilə bağlı apardığı araşdırmaya əsasən, sorğuda iştirak edən İT mütəxəssislərinin 43%-i bizneslərinin sosial mühəndislik

hücumlarına məruz qaldığını, 48%-i isə hər bir sosial mühəndislik hücumunun onlara orta hesabla 25.000 dollara başa gəldiyini bildirib [1, s.18].

İnstitusional olaraq görüləcək kiçik tədbirlər milli kibertəhlükəsizliyə əhəmiyyətli töhfələr verə bilər. Bu tədbirlərdən biri də dövlət və özəl qurumlarda başlanmış İT layihələrinə təhlükəsizlik elementinin əlavə edilməsidir. Bundan başqa, həm normal istifadəçilər, həm də qurumların İT personalı üçün standart əməliyyat siyasətlərinin yaradılması və bu standartların icrasına nəzarətin gücləndirilməsi sistemlərin təhlükəsizliyinə təhdidlərin xeyli hissəsini aradan qaldıracaqdır. İlk növbədə, ictimai və kritik sektorlarda istifadə olunan aparat və proqram təminatı sınaqdan keçirilməli və onların təhlükəsizliklə bağlı zəiflikləri gözardı edilməməlidir. Çünki sistemlərin əsas elementləri olan aparat və proqram təminatında baş verə biləcək zəifliklər alınacaq tədbirləri əvvəldən qeyri-funksional edəcəkdir.

İnstitusional əhəmiyyət kəsb edən digər məsələ qurumlararası əməkdaşlıqdır. Xüsusilə kibertəhlükəsizliyə cavabdeh olan qurumlar arasında sürətli məlumat mübadiləsi və əməkdaşlıq bu qurumların effektivliyinə müsbət təsir göstərəcəkdir [2, s.56].

Təkcə dövlət qurumları arasında məlumat mübadiləsi və əməkdaşlıq deyil, həm də dövlət və özəl sektor arasında məlumat mübadiləsi və əməkdaşlıq mexanizmlərinin yaradılması çox vacibdir. Belə bir əməkdaşlıq ictimaiyyət üçün xüsusilə faydalı olardı. Çünki dövlət informasiya sistemlərinin əhəmiyyətli bir hissəsi özəl sektor tərəfindən idarə olunur.

İnformasiya texnologiyası prosesin manipulyasiyanın və biliklərin idarə edilməsi vasitəsi kimi istifadənin predmetidir. İstifadə nümunələri internet, radio və başqalarıdır.

Rabitə texnologiyası məlumatların bir cihazdan digərinə paylanması və ya yayılmasının dəstəklənməsi prosesi ilə əlaqəlidir. İstifadə nümunələri kimi telefon dəstləri, mobil telefonlar və s. göstərilə bilər. Müasir dövrdə, demək olar ki, bütün texnologiyalar, xüsusilə də informasiya-kommunikasiya texnologiyaları davamlı inkişaf edir. Gündəlik həyatda çox önəmli olan informasiya-kommunikasiya texnologiyalarının təhsil sahəsində də rolu və mövqeyi nəzərə alınaraq, bu sahəyə daha çox tətbiq edilməlidir.

İnformasiya və kommunikasiya texnologiyalarının məcmusu olan İKT informasiyanın bir cihazdan digərinə göndərilməsi və ya ötürülməsinə yönəldiyindən məlumatın emalı, manipulyasiyası və istifadəsi ilə bağlı subyekt kimi müəyyən edilə bilər. İKT-nin yaranmasına səbəb olan amillərdən biri də XX əsrdən başlayaraq kompüterləşdirilmiş texnologiyanın inkişafıdır.

Elektron idarəetməyə keçid prosesi üçün başlıca təklif təhlükəsizlik pozuntularının və zəiflik risklərinin minimuma endirilməsində təhlükəsizliyi təmin edən xidmət və həllərin işlənib hazırlanmasıdır. İKT və kibertəhlükəsizlik sahəsində mövcud qanunvericilik bazasını nəzərə alan sistemləri əvvəldən layihələndirmək daha ucuz və asandır.

Hər il oktyabr ayı ABŞ və Avropa ölkələrində "Kibertəhlükəsizliklə bağlı maarifləndirmə ayı" kimi qeyd olunur və İKT ilə bağlı müxtəlif tədbirlər təşkil edilir. Hesab edilir ki, milli səviyyəli seminarların və praktiki məşğələlərin keçirilməsi hüquq-mühafizə şöbələri və insidentlərə cavab verən qruplar tərəfindən kibercinayətkarlıqla mübarizə sahəsində əks-tədbirlərin hazırlanması və təqdim edilməsində təsirli olacaqdır.

Vətəndaşlara əsas kibertəhlükəsizlik bacarıqları toplusunu və biliklərini çatdırmaq üçün texnika və alətlər, həmçinin kiberinsidentlərin müəyyən edilməsi və məlumatlandırılması ilə bağlı kütləvi informasiya vasitələrində kampaniyalar təşkil edilməlidir.

Ümumiyyətlə, ölkənin kibertəhlükəsizliyə davamlılığının artırılması milli strategiyalardan və idarəetmədə düzgün kibertəhlükəsizlik təminatından asılıdır. Bütün mövcud tədbirlər avadanlıq və proqram təminatı, kibertəhlükəsizlik üzrə ekspertlər və vaxt kimi resurslar tələb edir.

## Nəticə

Kibercinayətkarlıq formalarının dəqiq müəyyənləşdirilməsi informasiya texnologiyaları sahəsində insanların sərbəst və təhlükəsiz şəkildə yaşaması və fəaliyyət göstərməsi üçün olduqca vacibdir. Transmilli xarakterinə və nəticələrinin ciddiliyinə görə digər beynəlxalq cinayətlərdən, bəlkə də, daha təhlükəli olan kibercinayətkarlıq aktual hüquqi məsələ kimi nəzərdən keçirilməlidir. Müvafiq qurumlar

bu sahədə təbliğat işləri aparmalı, təlim və maarifləndirici materialların ictimaiyyətə çatdırılması, o cümlədən biliklərin yayılması, radio, televiziya və internet resurslarından istifadə edilməsi, normativ-hüquqi bazaların kütləvi informasiya vasitələrində geniş tətbiqinə kömək etməlidirlər.

Nəzərə almaq lazımdır ki, kiberməkandan istifadə, o cümlədən informasiya ehtiyatlarının mühafizəsi və kibercinayətkarlığa qarşı mübarizə milli təhlükəsizlik qədər mühümdür. Kiberhücumlarına məruz qalan şirkətlərin hücum müddətindən sonra səhm qiymətləri və gəlirlərində statistik fərqlərin olduğu və hücumların şirkətlərin fəaliyyətinə birbaşa təsir etdiyini söyləmək olar. Potensial səhmdarlar şirkət məlumatlarının sındırılması nəticəsində yaranan təhlükəsizlik və sabitliyin pozulması səbəbindən şirkətə investisiya qoymaqdan çəkinə bilər.

Kibertəhlükəsizliyin zəif təşkili maliyyə analitiklərini, investorları və kreditorları narahat edən səbəblərdəndir. Çünki bu, şirkətin bazar dəyərinin azalmasına gətirib çıxara bilər. Kibercinayətkarlıq şirkət üçün daxili nəzarət məsələsidir. Şirkətlər uğurlu biznesə sahib olmaq, öz biznes məlumatlarını və əməliyyatlarını qorumaq üçün güclü daxili nəzarətə ehtiyac duyurlar.

Kibertəhlükəni dəqiq ölçmək və strategiya hazırlamaq üçün müşahidə, təqib, təhlil və proqnozlaşdırma qabiliyyətinə malik bölmələrə ehtiyac vardır. Təkcə internet şəbəkələrini deyil, bütün kommunikasiya infrastrukturlarını əhatə edən kibertəhlükəsizlik siyasəti müəyyən edilməlidir.

Terror təşkilatlarının potensialı nəzərə alınaraq, passiv müdafiə ilə yanaşı, aktiv müdafiə üçün də tədbirlər görülməlidir. Kibertəhlükəsizlik sahəsində tədbirlər hazırlanarkən təhlükəsizlik-demokratiya, fayda-xərc balansı da nəzərdən qaçırılmamalıdır.

Kibercinayətkarlıqla mübarizə üzrə hüquqi infrastruktur mökəmləndirilməlidir. Kiberterrorizmlə qanunun aliliyi çərçivəsində mübarizə aparmaq üçün konsepsiya müəyyən etmək və bu cür fəaliyyətlərə görə sanksiyalar hazırlamaq lazımdır. .

Son onilliklərdə İKT texnologiyalarının sürətli inkişafı, eləcə də internet istifadəçilərinin sayının artması baxımından elektron dövlət quruculuğu sahəsində regionun lider dövlətlərindən olan Azərbaycanda kibercinayət və kibertəhlükəsizlik məsələləri dövlətin strateji prioritetləri sırasındadır. Ölkə rəhbərliyinin bu sahədə müvafiq qanunverici əsasların hazırlanmasına, infrastrukturun yaradılması və inkişafına həssas diqqəti göz önündədir.

Son illərdə kibercinayət və kibertəhlükəsizlik məsələlərinin gündəmə çevrilməsi, Azərbaycanda ümumilikdə əhalinin və sahibkarlıq subyektlərinin kibercinayət cəhdləri ilə üzləşməsi və ya ondan zərər çəkməsi, eləcə də kibertəhlükəsizliyə dair aidiyyətli qurumların real və potensial imkanlarının dəyərləndirilməsi bu sahədə geniş tədqiqatları zəruri etmişdir.

Reallıq bundan ibarətdir ki, dövrümüzün ən böyük problemlərinin həlli və çıxış yolları Azərbaycanda da məhz birgə və ortaq səylər tələb edir. Cəmiyyətimizin mövcud kibertəhdidlərlə bağlı dünyagörüşü və maarifləndirilməsi, təhlükələrə qarşı çevik reaksiya sərgiləməsi və hazırlığı sahənin peşəkarlarının, dövlət qurumları və özəl sektorların, o cümlədən akademik ictimaiyyətin bir araya gəlməsi təmin edilmədən mümkün deyil.

## İstifadə edilmiş ədəbiyyat siyahısı

1. Кардава, Н.В. Киберпространство как новая политическая реальность: вызовы и ответы // История и современность, – 2018. № 2, – с. 152–166
2. Məcidli, S.T. Kibercinayətlər// – Bakı, 2019.– 314 s.
3. Number of internet and social media users worldwide as of January 2023(in billions): [Electronic resource] / URL:https://www.statista.com/statistics/617136/digital-population-worldwide/
4. The Global Risks Report 2018[Electronic resource] / URL: https://www.weforum.org/reports/the-global-risks-report-2018/
5. Collin, B. The Future of Cyberterrorism // – Crime & Justice International Journal – 1997.Vol. – p.13–142.
6. Krasavin, S. What is Cyber-terrorism? [Electronic resource] / Computer Crime Research Center (CCRC). – URL: http://www.crime-research.org/library/Cyber-terrorism.htm

7. Голубев, В.А. Кибертерроризм – Угроза национальной безопасности: [Электронный ресурс] / URL: www.crive-research.ru
8. Карамова, Э. Фомин С. К вопросу о кибертерроризме в глобализирующемся мире // Социально-политические науки. – 2016, №3.– с. 154-155.
9. Овчинский, В.С. Криминология цифрового мира: учебник для магистратуры / В. С. Овчинский. – Москва: Норма: ИНФРА-М, 2018. – 417 с.
10. Старостина, Е.В., Фролов Д.Б., Защита от компьютерных преступлений и кибертерроризма Вопросы и ответы. [Электронный ресурс]// URL: http://kursak.net/kiberterrorizm-i-osobennosti-ego-proyavleniya/
11. . Соколов, А.В. Информационное общество в виртуальной и социальной реальности. – СПб Алетейя, 2012. – 385с
12. Гаврилов, Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю.В.Гаврилов, Л.В. Смирнов. – М.: ЮИ МВД РФ, 2003. – 477 с.
13. Ahlgren, M. Cybersecurity statistics and trends: [Electronic resource] / – 2016, Febraury 2. URL: https://www.websiterating.com/research/cybersecurity-statistics-facts/
14. Öztürk, E., Ateş, A., Erdoğan, B. Siber suçların hukuksal yönleri ve psikolojik dinamikleri// Türkiye Klinikleri,– 2020. Aralık, – s. 48-55.

**Аннотация**
**Новый глобальный тренд: угроза кибертерроризма растет**
**Захид Орудж**

В статье кратко рассматривается история возникновения и развития кибертерроризма, анализируется понятие кибертерроризма как нового глобального тренда угроз, распространяющегося в современную эпоху, рассматриваются его научная природа и характеристики, а также место и роль в статистике киберпреступлений. Уделяется внимание вопросам, связанным с организацией киберзащиты в современную эпоху широкого распространения международного кибертерроризма. На основе международного опыта рассматриваются и анализируются последствия, вызванные кибертерроризмом и кибератаками, опасности, которые они представляют, и пути их устранения.

На основе системного подхода явление кибертерроризма оправдывается как угроза безопасности международного сообщества и национального государства, а также как одно из наиболее эффективных средств достижения политических целей во всем мире. Подчеркивая, что кибертерроризм станет самым опасным оружием и будущем, изучаются пути защиты от него.

В статье на основе исследовательских источников определяются актуальные направления, связанные с актуальными проблемами борьбы с компьютерным терроризмом в современном обществе. Затронуты приоритетные формы межгосударственного сотрудничества, а также отмечены необходимые меры, направленные на повышение эффективности борьбы с кибертерроризмом.

**Ключевые слова:** киберпреступность, правовые аспекты, кибербезопасность, национальное законодательство, международное законодательство, правовая борьба, Азербайджан

**Abstract**
**A new global trend: Against the backdrop of growing cyberterrorism threats**
**Zahid Oruj**

The article briefly reviews the history of the emergence and development of cyberterrorism, the concept of cyberterrorism is analyzed as a new global threat trend that is spreading in modern times, its scientific nature and characteristics, as well as its place and role in the statistics of cybercrimes are reviewed. Attention is paid to issues related to the organization and implementation of cyber defense in

the current era of widespread international cyber terrorism. The consequences caused by cyber-terrorism and cyber attacks, the dangers they pose and ways to eliminate them are examined and analyzed based on international experience.

Based on a systematic approach, the phenomenon of cyber-terrorism is justified as a threat to the security of the international community and the nation-state, and as one of the most effective means to achieve political goals worldwide. Emphasizing that cyber terrorism will become the most dangerous weapon in the future, ways to protect against it are being explored.

In the article, current directions are determined based on research sources related to the actual problems of the fight against computer terrorism in modern society. The priority forms of interstate cooperation are touched upon, as well as the necessary measures aimed at increasing the effectiveness of the fight against cyber-terrorism are noted.

**Keywords:** cybercrime, legal aspects, cyber security, national legislation, international legislation, legal struggle, Azerbaijan

*Məqalə redaksiyaya daxil olmuşdur:25.07.2023*
*Təkrar işlənməyə göndərilmişdir:26.01.2024*
*Çapa qəbul edilmişdir: 19.02.2024*