UOT: 34.343 **DOI: 10.34826/NAA.2023.25.1.009**

KİBER TERRORİZM: ONUN RİSKLƏRİ, TÖRƏDİLMƏ VƏ MÜBARİZƏ ÜSULLARI, ƏNƏNƏVİ TERROR AKTLARINDAN FƏRQLƏRİ

Musayev E.H.
Bakı Dövlət Universiteti

Elm və texnologiyaların sürətli inkişafı nəticəsində artıq transmilli cinayətlərin də rəqəmsallaşması müşahidə edilməkdədir. Bu cinayətlərdən biri də yeni nəsil terror-kiberterror cinayətləridir. Artıq termin kimi kiber terrozim və kiber terrorun cəmiyyət tərəfindən yadırğalanmadan qəbul edilməsi qlobal olaraq bəşəriyyətin cinayətlərin rəqəmsallaşmasına təbii prosess kimi yanaşmasının təzahürüdür.

Bu da özlüyündə digər kibercinayətlər kimi kiber terrorun da araşdırılmasının və ona qarşı mübarizə yollarının tədqiq edilməsinin labüdlüyünü və aktuallığını göstərir.

Məqalədə kiber terrorizmlə bağlı anlayışlara, o cümlədən "white collar terrorist" terminina aydınlıq gətirilmişdir. Həmçinin, kiber terrorun ənənəvi terrora görə fərqli və üstün cəhətləri, potensial törədilmə üsulları, kiber terrorizmlə bağlı fərqli nəzəriyyələr, kiber terrorun dövlət qurumlarına və onun informasiya sistemlərinə hansı dərəcədə təhdid olması haqqında nəzəri məlumatlar yer almışdır.

Kiber terrorizmlə mübarizə yolları, onların effektivlik dərəcəsi, bu cinayətlə onlayn və ənənəvi medianın, kiv-lərin əlaqəsi də məqalədə qeyd edilmişdir.

Açar sözlər: *kiber terrorizm, kiber terrorist, kiber terror, informasiya sistemləri, "ağ yaxalıqlı terrorist", rəqəmsal media, kiber hücum.*

Kiber terrorizm son on ildə çap mediası və sosial mediada tez- tez rastlaşdığımız, dünya gündəmində yer alan bir anlayışdır. Kiber terrorizm informasiya sistemləri əsasında elektronik vasitələrin, kompüter proqramlarının ya da digər elektronik ünsiyyət formalarının istifadə edilməsi ilə qlobal balans və milli maraqların qarşısının alınmasını hədəfləyən şəxsi və ya siyasi motivdə məqsədyönlü hərəkət və fəaliyyətdir. Qısaca, kiber terrozim dedikdə, klassik terror aktlarının kompüter və kompüter sistemlərindən istifadə olunaraq icra edilməsi nəzərdə tutulur.

Kiber terrozim anlayışı onun məqsəd və vasitələri prizmasından belə müəyyən edilmişdir: "Xalq içində qorxu yaratmaq və əsas dövlət qurumlarına xalqın inamını sarsıtmaq məqsədi ilə məlumatların mühafizə edilməsi və xidmətlərin göstərilməsi sahəsində kütləvi narazılığa səbəb olmaq üçün kompüter kodlarını və əlaqəli qurğu və proqramları istifadə etməkdir" [1].

Digər bir mənbədə kiber terrozim daha geniş formada anlayış kimi izah olunur. Sözügedən mənbədə qeyd olunur ki, kiber terrorizm kiber uzay və terrozimin birləşməsidir. Kiber terrozim dedikdə, ümumi olaraq kompüterlərə, şəbəkələrə və bunlarda qorunan məlumatlara yönəlmiş qeyri-qanuni hücumlar və siyasi, yaxud sosial məqsədlərə çatmaq üçün hökumət və ya bir qrup işçilərə təzyiq göstərmək və qorxutmaq məqsədi ilə edilən hücum hədələri başa düşülür. Lakin obyektiv baxımdan hər hansı cinayət əməlinin kiber terrozim kimi müəyyənləşdirilməsi üçün həmin əməlin şəxsə, yaxud mülkiyyətə qarşı şiddətlə nəticələnməsi və ya ən azından qorxu yaradacaq qədər zərərverici olması lazımdır. Ölüm, yaxud yaralanma ilə nəticələnmiş hücumlar, partlayışlar, təyyarə qəzaları, suların çirklənməsi kimi ekoloji, yaxud ciddi iqtisadi itkilər nümunə kimi göstərilə bilər. Kritik infrastruktur sistemlərinə qarşı olunan terror aktları səbəb olduğu nəticələrdən asılı olaraq kiber terrorizm adlandırıla bilər.

Hər hansı bir cinayətin kiber terrorizm kimi dəyərləndirilməsi üçün vacib olan ünsürləri nəzərə alsaq kiber terrorizm terminina göstərilən kimi anlayış verə bilərik: "Siyasi, sosial və ideoloji məqsədlərə nail olunması üçün bir terror təşkilatı tərəfindən həyata keçirilən, cəmiyyətdə dəhşət və qorxu yaradan, hədəfi informasiya sistemləri tərəfindən nəzarət edilən kritik infrastruktur sistemləri və ya birbaşa olaraq xüsusi əhəmiyyət kəsb edən informasiya sistemlərinin özü, istifadə etdiyi vasitənin də yenə informasiya sistemləri olan, təsir baxımından klassik terror aktına bərabər nəticələr doğuran hər növ qeyri-qanuni hücum və hücum hədəsidir."

Burada nəzərdə tutulan kiber terrorizmin məqsədi özündə dövlət və ya cəmiyyətyönümlü mesajları ehtiva etməkdir. Kiber terroristlərin hədəflərində həmçinin şirkətlər, üçüncü şəxslər və iqtisadi qurumlar da ola bilər.

Həm informasiya sistemləri vasitəsilə törədilən ənənəvi terror aktları, həm də informasiya sistemlərindən istifadə etməklə elə bu sistemlərə və ya ehtiva etdiyi məlumat, yaxud da sistemin işləmə qaydasına qarşı edilən aktlar – bunların hər ikisi kiber terror anlayışına daxil edilir.

Kiber terrorizm yeni baxışlara rəqəmsal və araşdırmalara açıq bir sahədir. Belə ki, informasiya sistemləri və sosial media cari zaman üçün daha çox təbliğat və terrorizmin maliyyələşdirilməsi üçün istifadə edilir kimi görünsə də, əslində təyyarələrin uzaqdan idarə edilməsi, bomba istehsalı, müxtəlif kodların deşifrə olunması, dövlət üçün gizli qalması vacib olan informasiya ehtiyatlarına daxil olmaq kimi terror aktlarına faydalı olacaq, yaxud bu aktlarda istifadə ediləcək məlumatların da əldə edilməsi mümkün olan virtual mühitlərdir. Kiber terroristlər tərəfindən informasiya sistemləri, yaxud kompüter və internet şəbəkələrindən istifadə edilməklə bir şəhərin işıqforlarının dondurulması, telefon rabitəsinin iflic vəziyyətə gətirilməsi, əhalinin elektrik və təbii qazla təminatının dayandırılması, informasiya sistemlərinin özünün işləməsində nasazlıqların yaradılması və bu sistemlərə girişin məhdudlaşdırılması, ictimai nəqliyyatın qrafikinin dəyişdirilməsi və pozulması, bank və maliyyə sektorunda müəyyən məhdudiyyətlər, polis, təcili yardım və yanğınsöndürmə ilə bağlı fəaliyyətin pozulması, dövlət orqanlarının normal fəaliyyətinin pozulması, bloklanması və s. kimi digər hərəkətlər törədilə bilər.

Kiber terrorda terroristlər tərəfindən törədilən aktları xarekterinə görə iki qrupa bölmək olar:

1) Zorakı aktlar. Zorakı aktlar dedikdə, dövlətlərin və millətlərin ortadan qaldırılmasına, yaxud digər siyasi və s. məqsəd güdən, lakin eyni fiziki yolla da törədilə bilən klassik terror aktlarına bənzər aktlar başa düşülür.

2) Qeyri-zorakı aktlar. Qeyri-zorakı terror aktlarına isə internet üzərindən təşkilat üzvlərinin bir- biriləri ilə əlaqə qurmaları və yenə internet üzərindən bomba istehsalı və ondan istifadə qaydaları, silahdan istifadə haqqında məlumatları, cinayətkarın tutulması halında istintaq orqanında ifadələrin alınması zamanı davranış barədə təlimləri, hər hansı canlı/cansız obyektə münasibətdə şiddət və nifrət ehtiva edən fikirləri cəmiyyətə və onlara rəğbət bəsləyən kütləyə çatdıraraq məqsədləri üçün ictimai rəy formalaşdırıb təbliğat ilə məşğul olmağı və ya manipulyativ fəaliyyət göstərməyi misal gətirmək olar [3].

Kiber terrorizmin yayılması ilə əlaqədar bizim dilə "ağ yaxalıqlı terrorist" kimi tərcümə olunan "white collar terrorist" termini də yeni yaranmışdır. Bu qrup terroristlər əslində cəmiyyətdən təcrid olunmayan, əksinə cəmiyyətlə iç-içə yaşayan, yaxşı təlim keçmiş, o cümlədən informasiya texnologiyaları mövzusunda kifayət qədər məlumatları olan və o sahədəki boşluqlardan özü, yaxud üzv olduğu təşkilatın çıxarları naminə istifadə etməyi bacaran şəxslərdir. Bu şəxslərin faktiki və fiziki olaraq sağlamlıqları və yaşamları yüksək risk altında olmadığından və tutulma riskləri az olduğundan klassik terroristlərlə müqayisədə uzunmüddətli fəaliyyət göstərə bildiyi üçün daha təhlükəlidir [2, I cild].

Ümumiləşdirsək deyə bilərik ki, bir professional "ağ yaxalıqlı" terrorist onlarla, bəlkə də yüzlərlə ənənəvi terroristi əvəz edə bilər.

Kiber terror barədə digər maraqlı mövzu isə kiber terrorun ənənəvi terrora görə bir çox perspektivlərdən üstünlükləri və fərqlərinin olmasıdır. Bunlardan bir neçəsi aşağıdakılardır:

1. Həyat təhlükəsizliyi. Terror təşkilatları klassik üsullarla terror aktları törədən zaman üzvlərinin həyatı böyük təhlükə ilə üz-üzə qalır və bir çox hallarda həyatlarını itirirlər. Əlində silah, yaxud bomba olan terroristin həyatı həmin akt zamanı ya mühafizə qüvvələrinin gördüyü tədbirlər, yaxud da elə özünün törətdiyi hadisə nəticəsində (üzərində olan bombanı partlatması, silahlı akt zamanı sonda özünə atəş açması və s.) sonlanır. Lakin dünyanın istənilən bir yerindən müvafiq informasiya sisteminə, yaxud internetə və s. şəbəkəyə qoşulan kiber terrorist öz həyatını heç bir təhlükəyə atmadan terror aktını törədərək əldə etmək istədiyi nəticəyə nail olur və məqsədini gerçəkləşdirir.

2. Terror aktının əsl məqsədi. Ənənəvi qaydada törədilən terror aktlarının əsas məqsədi bir qayda olaraq hədəf aldığı siyasi rejimə və ya cəmiyyətə mesaj verməkdir (məsələn, bir müsəlman

terror təşkilatı tərəfindən məscidlərin partladılmasında məqsəd məscidə, yaxud orda ibadət edən şəxslərə ziyan vermək deyil, həmin ərazidə hökm sürən siyasi rejimə, yaxud müəyyən toplumlara mesaj göndərməkdir). Yəni, klassik terrorda şiddət göstərmək və ziyan vurmaq vasitədir. Yeni nəsil terrorda isə müvafiq olaraq "virtual şiddət" bir vasitə deyil, məqsəd qismindədir. Məsələn, informasiya texnologiyalarından istifadə etməklə ağ yaxalıqlı terrorist böyük bankların, maliyyə qurumlarının və fond bazarlarının məlumatlarına girişi və onlarla əlaqəni məhdudlaşdıraraq nəticədə böyük iqtisadi zərərlərə səbəb ola bilər. Sözügedən misalda hər hansı ölkənin iqtisadı həyatı iflic həddinə çata bilər, o cümlədən iqtisadi böhranın ortaya çıxması gözlənilə bilər. Eyni misalı qida və dərman preparatlarının istehsalı sahəsində də çəkə bilərik. Bu misalda da, nəticə etibarı ilə dövlətə və cəmiyyətə böyük zərər vurula bilər. Hər iki nümunədə biz törədilməsi planlanan, yaxud törədilən terror aktında əsas məqsədin ziyan və zərər vurulması olduğunu görürük.

3. Lokallıq və qloballıq. Ənənəvi terror aktında baş vermiş hadisə, edilmiş təbliğat barədə məlumat geniş kütlələrə, demək olar ki, dünyanın hər yerindən olan insanlara çatır. Lakin burada diqqət edilməli nüans ondadır ki, məlumat qloballaşsa da, akt özü lokal xarekter daşıyır və ərazi baxımdan konkretdir. Məsələn, bir dövlət binasının partladılması nəticəsində bina çökə bilər və içindəki insanlar həyatlarından ola bilərlər, bu akt barəsində xəbərlər isə bütün dünyada yayıla bilər. Burada göründüyü kimi akt özü lokaldır və konkretdir. Ancaq kiber terrorizmdə aktın təsir ərazisinin genişləndirilməsi mümkündür. Belə ki, müəyyən kodların yığılması və kompüterdə, yaxud digər elektronik cihazda müvafiq düymənin sıxılması ilə bir və ya bir neçə dövlətə aid müxtəlif kateqoriyadan olan minlərlə internet saytları eyni anda çökə bilər və yaxud bir internet saytı bir və ya bir neçə ölkədə eyni anda fəaliyyətsiz qala bilər. Onu da qeyd edək ki, kiber terrorist tərəfindən eyni anda bir neçə terror aktı törədilə bilər və bu aktlar ərazi baxımından lokal olmadığı və bir neçə ölkəni əhatə etdiyi (azı 2) təqdirdə kiber terrorizmin trasnmilli cinayət olduğu qənaətinə də gələ bilərik.

4. Psixoloji təsir və reaksiya. Kiber terrorun təsiri informasiya sistemləri ilə əlaqəli şəkildə məhdudlaşdığı və hədəflərin özlüyündə simvolik xarekter daşımadığı səbəbi ilə, kiber terror ənənəvi terror aktları qədər yayılmayacaqdır. Həmçinin kiber terror aktları nəticəsində insanların ölməsi və yaralanması hallarının demək olar ki, müşahidə olunmaması səbəbindən ictimai rəyin reaksiyası da radikal mövqedən olmayacaqdır [2, III cild].

5. Yaş həddi problemi. Ənənəvi terror aktlarında fiziki gücün üstünlük təşkil etməsi və terrorların psixoloji hazırlanması və s. digər səbəblərə görə seçilən militantlara münasibətdə bir qayda olaraq müəyyən yaş həddi senzurası tətbiq olunur. Lakin kiber terror aktlarını yeniyetmə yaşına çatmayan şəxslər belə törədə bilirlər. Bu da, özlüyündə bu cinayətin istintaqı zamanı təqsirləndirilən şəxslərin məsuliyyətə cəlb edilməsi məsələsində kifayət qədər problemlərə gətirib çıxara bilir.

6. Təchizat və təminat. Kiber terroristlər klassik terroristlərdən fərqli olaraq terror aktlarını törətmək üçün bombalara, silahlara və s. ehtiyac duymur. Həmin şəxslər üçün lazımi təchizat kompüter və ya digər oxşar elektronik cihazlar və şəbəkə bağlantılarından ibarətdir. Nəticə etibari ilə yeni nəsil terroristlər terror aktını daha az risk, daha az maliyyə xərci ilə, o cümlədən məkan və zaman məhdudiyyəti olmadan həyata keçirə bilirlər.

7. Cinayətdə icraçılıq və risk faktoru. Ənənəvi terror aktlarında aktın törədilməsində icraçı şəxs qismində iştirak edənin tutulması riskinin böyük olması səbəbi ilə çox vaxt icraçılar elə terror təşkilatının üzvlərindən seçilirlər. Kiber terror aktlarında isə icraçı qismində professional hakerlərdən istifadə edilməsi risk səviyyəsinin minumuma endirilməsinə gətirib çıxarır. Bu praktikadan istifadə terror aktını törədən şəxsin terror təşkilatının üzvü olmaması səbəbindən istintaq zamanı təhrikçilərin müəyyənləşdirilməsində, həmçinin planlanmış terror aktı barədə əvvəlcədən məlumat əldə edilməsində hüquq mühafizə orqanlarına ciddi çətinliklər törədir [2, III cild].

Texnologiyanın sürətlə inkişaf etdiyi bu dövrdə kiber cinayətlərin də statistikasında ciddi artım müşahidə edilir. Bu artımın müəyyən qismi də kiber terrorun üzərinə düşür. Digər kibercinayətlərə nisbətən az yayılmış kiber terrorun gələcəyə münasibətdə dinamik artımı ehtimal

edilir. Ümumi olaraq yeni nəsil olan rəqəmsal hüquq çərçivəsində kiber terrorun gələcəyi barədə bir-birinə zidd iki nəzəriyyə aktuallıq daşıyır.

Birinci nəzəriyyədə sözügedən terror aktlarının həyata keçirilməsinin çətin olduğu, bu baş versə belə riskin süni olaraq böyüdüldüyü, böyükmiqyaslı, təlaş və qorxu yarada biləcək kiber terror hücumlarının həyata keçirilməsinin mümkün olmadığı qeyd olunur. Bugünə qədər terror təşkilatları tərəfindən və yaxud fərdi olaraq hərəkət edən terroristlər tərəfindən kritik infrastruktura qeyd olunan formada genişmiqyaslı və koordinasiyalı hücumun olmadığı göstərilir.

İkinci nəzəriyyədə isə, informasiya texnologiyalarının inkişafı ilə birlikdə kiber terror təhdidinin hər gün artması və bugünədək qeyd olunan cinayətin törədilməməsinin gələcəkdə də belə halın olmamasını istisna etməməsi vurğulanır.

Kiber terror və təhlükəsizlik məsələləri ilə maraqlanan bir sıra mütəxəssislər kiber terrorun ciddi təhdid olduğunu, irimiqyaslı kiber terror hadisəsinin nəticələrinin əvvəlcədən öngörülməsinin çətin olduğunu, böyük iqtisadi zərər, qorxu və canlı qüvvə itkisinə səbəb ola biləcəyini, o cümlədən informasiya texnologiyalarının dinamik inkişafındakı irəliləyiş ilə paralel olaraq təhlükənin də eyni formada artdığını qeyd edirlər [2, II cild].

Bu cinayətin potensial törədilmə üsullarına aşağıdakıları nümunə gətirmək olar:

1. Dərman istehsalı ilə məşğul olan şirkətlərin informasiya sistemlərinə qanunsuz olaraq müdaxilə edilərək dərman preparatlarının və tərkibinin siyahısının dəyişdirilməsi. Kütləvi olaraq insan ölümü, əlilliyin yaranması və ya ən yüngül halda insanların xəstələnməsi ilə nəticələnə bilər.

2. Hər hansı bir şəhərin, yaxud ərazinin işıqforlarını tənzimləyən, yaxud qatarların istiqamətlərindən siqnalizasiya sisteminə müdaxilə edilməsi çoxsaylı qəzalar və insan ölümləri və ya yaralanmalarına səbəb ola bilər.

3. Qida fabriklərinin istehsalı ilə bağlı informasiya sistemlərinin ələ keçirilərək qida komponentlərinin miqdarı və nisbətində dəyişiklik edilməsi. Bu yolla istər daxili istehlak, istərsə də ixracat üçün nəzərdə tutulmuş malların istifadə edilməsi nəticəsində bir və ya bir neçə ölkədə kütləvi ölümlər, zəhərlənmələr və s. kimi hadisələr baş verə bilər.

4. Hava nəqliyyatının idarəetmə sistemlərinə hücum edilərək, kommersiya, hərbi, yaxud sərnişindaşıma fəaliyyətini həyata keçirən hava gəmilərinin bir- birilə toqquşmasına, qəzaya uğramasına və ya hədəflənən yerə çatmamasına səbəb ola bilər. Bu misal dəmir və dəniz yollarına da şamil oluna bilər [2, II cild].

5. Bankların, beynəlxalq maliyyə sistemlərinin, birjaların informasiya sistemlərindəki məlumatların əlçatanlığının məhdudlaşdırılması və ya həmin məlumatların silinməsi, yaxud istifadəyə yararsız vəziyyətə gətirilməsi nəticəsində həm istifadəçilərə ziyan verilməsinə, həm xidməti təklif edən sistemlərin işinin pozulmasına, həm də şəxslərin iqtisadi sistemə inamının sarsılmasına səbəb ola bilər [2, II cild].

6. Bir və ya bir neçə xəstəxananın informasiya sisteminə müdaxilə edilərək xəstələrin qeydiyyatı aparılmış bölmədə məlumatların silinməsi, vahid sistemdən idarə olunan avadanlıqların fəaliyyətinin pozulması, analiz nəticələrinin dəyişdirilməsi nəticəsində insan ölümlərinə, müalicələrinin uzanmasına və s. digər fəsadlara yol açma.

7. Elektrik xətləri, qaz və neft boruları, su anbarları və s. kimi kritik əhəmiyyətə sahib təsisatlara qarşı kiber hücumlar edilərək kütləvi partlayışlara, ölümlərə səbəb olma və s.

Bu nəticəyə gələ bilərik ki, kiber terror aktları bir ölkə əhalisinin qidalanmasına və yaşamaq üçün mühim digər funksiyalarının pozulmasına səbəb ola biləcək potensialdadır. Bu da, özlüyündə kiber terrorun təhlükəlilik risk faktorunun son dərəcə yüksək olduğunun göstəricisidir.

Rəqəmsal dünyada sürətin önəmli faktorlardan biri olması kiber terroristlər üçün niyyətlərini həyata keçirmək və yaymaq üçün əlverişli şərait yetişdirir.

Belə ki, bu faktor medianın kiber terror təşkilatlarına və kiber terrora olan marağı ilə birləşdikdə, baş vermiş terror aktı medianın da "köməyi" ilə saniyələr içərisində bütün dünyaya yayılır.

Törədilmiş aktda istifadə olunan üsul və aktın detalları və s. insanlar tərəfindən oxunur. Təbii ki, bu insanlar içərisində digər terror qruplaşmalarının üzvləri və s. digər cinayətkar şəxslər olur. Nəticədə, bəlkə də həmin üsulu və yolu bilməyən cinayətkar "medianın" dəstəyi ilə

məlumatlanmış olur və onlayn mətbuat əslində yeni kiber terrorun, yaxud digər kiber cinayətlərin baş verməsinə "köməklik göstərir" [4].

Qlobal olaraq elm və texnologiyanın sürətli inkişafı hal-hazırda yaşadığımız gerçək həyatla virtual həyatımızı günü-gündən bir-biri ilə daha sıx və mürəkkəb bağlarla əlaqələndirir. Bu da nəticədə kiber terror cinayətinin törədilməsi üçün münbit bir mühitin yaranmasına gətirib çıxarır. Əgər ki, gələcəkdə kompüter informasiya ehtiyatları və sistemləri daha etibarlı şəkildə qoruna bilməzsə, yuxarıda sadaladığımız potensial cinayətlərin baş verməsi heç də uzaq görünmür.

Bu səbəbdən də, hər bir dövlət öz milli (yerli) məlumat-informasiya baza sistemlərinin infrastrukturunun təhlükəsizlik məsələlərinə xüsusi diqqət yetirməli, gələcəyə hesablanmış baxışla həm texniki nüansları, həm də hüquqi tənzimləmələri və dəyişiklikləri indidən nəzərə almalıdır.

İstənilən cinayətdə olduğu kimi, həm kiber terrozim, həm də klassik terrorizmə qarşı mübarizə cinayət hüquq sisteminin ən vacib vəzifələrindən biridir. Effektiv üsullardan biri beynəlxalq əməkdaşlıqdır ki, buna nümunə olaraq Avropa Şurasının "Terrorçuluğun qarşısının alınması haqqında" Konvensiyanın qəbul edilməsidir. Bu və bunun kimi beynəlxalq normaların qəbul edilməklə yanaşı, onun praktiki olaraq tətbiq edilməsi nəticə etibarı ilə terrozimə qarşı mübarizədə vacib addımlar atılmasına səbəb olacaqdır.

Texnologiyanın kiber terroristlər tərəfindən fərdi istifadəsinin məhdudlaşdırılması prizmasından baxsaq, əslində profilaktik tədbirlər görülməsi üçün irimiqyaslı məhdudlaşdırılmaların mümkün olmadığı aydın şəkildə görünür. Mobil telefonlar, internet və sosial platformalar kimi hamı üçün əlçatan olan vasitələrdən istifadənin hər hansı cəmiyyətdə bütün fərdlərə münasibətdə tam məhdudlaşdırılması mümkün deyil. Burada ən effektiv yol sözügedən məhdudlaşdırılmanın hüquqa uyğun şərtlərdə və həddlərdə həyata keçirilməsidir.

Məsələn, şübhəli şəxslərə münasibətdə izlənərək onlar olduğu ərazidə lokal olaraq, yaxud onların istifadəsində olan texniki vasitələrdə məhdudlaşdırmanın tətbiq edilməsidir. Təbii ki, burada da çətinlik yaradan bir digər nüans kibercinayətkarların şübhəli şəxs qismində cəlb edilməsi məsələsidir. Yekunda bu nəticəyə gəlmək olar ki, cari vəziyyətdə bu üsul effektiv hesab olunmur.

Kiber terrorizm günümüzdə, ən çox da dövlət qurumlarının təhlükəsizliyinin qorunmasına təhdid kimi qəbul edilir. Təhlükəsizliyin təmin olunması üçün bu gün ölkəmizdə də istifadə olunan "internet" şəbəkəsinin təkmilləşmiş versiyası kiber terrorizmlə mübarizədə daha faydalı olacaqdır. Ancaq bu şəbəkə böyüdükcə sistemdə təhlükəsizlik boşluqlarının yaranması riski də artır, bu səbəbdən də həmin şəbəkənin təkmilləşməsi zəruri hal alır.

Digər bir üsul isə, dövlətlərin virtual aləmi müntəzəm olaraq nəzarətdə saxlamasıdır. Lakin, burada da cəmiyyətin həssaslıqla yanaşdığı fərdlərin konstitusion hüquq və azadlıqlarına (məlumat azadlığı, şəxsi həyatın toxunulmazlığı hüququ və s.) birbaşa müdaxilə edilməməsi nəzərə alınmalıdır. Bu səbəbdən də, qeyd edilən nəzarət formasının əhatə dairəsi və sərhədləri konkret olmalıdır.

Kiber terrozimlə mübarizə yollarından biri də adıçəkilən cinayətin təbliğinin qadağan edilməsidir. Burada da əsas yük media və kütləvi informasiya vasitələrinin üzərinə düşür. İctimai faydanı maddi gəlirlərdən üstün tutaraq media qurumları və kiv-lər kiber terrozimlə mübarizə etmək üçün bu mövzu barədə məlumatları işıqlandırarkən istəmədən də olsa "əməkdaşlıq" etməməli, təbliğə meyilli yox, tənqidə meyilli formada cəmiyyətə təqdim etməlidir [4]. Burada da diqqət edilməli məqam şəxslərin məlumat əldə etmə azadlığı ilə mətbuatın və jurnalistikanın hüquqlarının mümkün qədər az şəkildə məhdudlaşdırılmasıdır.

Daha sərt tədbir olaraq bəzi ölkələrdə ümumən mətbuatda intiharla bağlı xəbərlərin verilməsinin qadağan olunduğu kimi, bu cinayətlərlə bağlı xəbərlərin də yayılmasının qadağan edilməsi tətbiq edilə bilər. Lakin bu, hər cəmiyyətdə eyni dərəcədə müsbət, yaxud mənfi nəticə verməyəcəkdir.

Hər iki formanın düzgün tətbiq edilməsi üçün "karma" modelini nəzərdən keçirək: İngiltərədə "karma" modelindən istifadə edilir, yəni kütləvi formada yayılmaması lüzum görülən məlumatlar və ya xəbərlər barədə media qurumlarına, kiv-lərə əvvəlcədən məlumat verilir. Ancaq bu qərar həm media qurumları və kiv-lərin, həm də əlaqəli dövlət orqanlarının birgə təşkil etdiyi "şura" tərəfindən kollegial şəkildə, hüquq və qanunvericiliyə uyğun şəkildə qəbul edilməlidir [5].

Yekun nəticəyə gəlmək olar ki, mətbuat azadlığı və şəxslərin məlumat əldə etmək azadlığının qorunması və minumum həddə məhdudlaşdırılması çərçivəsində media qurumları və kiv-lərin qanunların tələblərinə riayət etməklə yanaşı, öz iradələri ilə də kiber terror əməllərinin təbliğ edilməməsi və bu barədə məlumatların düzgün işıqlandırılması istiqamətində işlər görməlidir. Qanun və vicdanlı yanaşma tətbiq olunduğu halda əksər üsullar son dərəcə effektiv olacaqdır. Sözügedən işlərin görülməsi internet xəbərləri və sosial media üçün də keçərlidir.

REFERENCES

1. Cyber Crime and Cyber Terrorism; (Robert W. Taylor, Eric J. Fritsch, Michael R. Saylor, William L. Tafoya), Pearson Puplisher, 2018.
2. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools and Applications-Vol 1,2,3; (Information Reso Management Association), Information Science Reference, 2020.
3. New Threats and Countermeasures in Digital Crime and Cyber Terrorism (1st edition); (Maurice Dawson, Marwan Omar), IGI Global Publisher, 2015.
4. Mass-Mediated Terrorism: Mainstream and Digital Media in Terrorism and Counterterrorism (3rd Edition), (Brigitte L. Nacos), Rowman & Littlefield Publishers, 2016.
5. https://unesdoc.unesco.org/ark:/48223/pf0000247074

CYBER TERRORISM: ITS RISKS, METHODS OF OCCURRENCE AND FIGHTHING, DIFFERENCES FROM TRADITIONAL TERROR ACTS

Musayev E.H.
Baku State University

Transnational offenses are already being digitized as a result of the quick advancement of science and technology. Cyber-terrorism offenses of the new age are one of these crimes. The unwavering acceptance of cyber terrorism and cyber terror by society as a term is a manifestation of humanity's approach to the digitization of crime as a natural process.

This in itself demonstrates the importance and urgency of investigating cyber terrorism and other cybercrime and exploring ways to combat it. The term "white-collar terrorist," among others, is defined in the piece as it relates to cyberterrorism. In addition, the article includes theoretical information about the different and superior aspects of cyber terrorism from traditional terrorism, possible criminal methods, different theories about cyber terrorism, and the extent to which cyber terrorism poses a threat to government institutions and information systems.

In the article, the ways of combating cyber terrorism, their degree of effectiveness, the relationship of online and traditional media, MM (mass media) to this crime were also mentioned.

Keywords: *cyber terrorism, cyber terrorist, cyber terror, information systems, "white collar terrorist", digital media, cyber attack.*

Rəyçi: f.r.f.d., dos. Şekili Ş.P.

Müəllif haqqında məlumat

Soyadı, adı, atasının adı	İş yeri	Vəzifəsi, elmi dərəcəsi, elmi adı	Əlaqə
Musayev Erkin Hümbət oğlu	Bakı Dövlət Universiteti	Hüquq fakültəsi, Cinayət hüququ və kriminologiya kafedrasının "Cinayət hüququ və kriminologiya; cəza-icra hüququ" ixtisası üzrə əyani doktorantı	musayev2022@gmail.com mob: (+994) 50 289 90 88 (+994) 51 925 02 22