Kibercinayətlərlə mübarizə: çətinliklər və imkanlar

Elvin Balacanov

Lids Universiteti, Lids, Böyük Britaniya və Şimali İrlandiya Birləşmiş Krallığı
lw11eb@leeds.ac.uk

***Xülasə*— İnformasiya-kommunikasiya texnologiyalarının (İKT) sürətli inkişafı və tətbiq miqyasının genişlənməsi kibercinayətkarlığın sayının və zərər vurma potensialının yüksəlməsi ilə müşayiət olunur. Eyni zamanda, İKT kibercinayətkarlıqla mübarizə sahəsində hüquq mühafizə orqanlarına müəyyən imkanlar təqdim edir. Bu məqalədə kibercinayətkarlıqla mübarizədə qarşıya çıxan yeni imkanlar və çətinliklər analiz edilir və mübarizənin efektivliyi və səmərəliliyinin təmin olunması üçün təkliflər irəli sürülür.**

Açar sözlər—İKT; kiberməkan; kibercinayət; araşdırma; elektron sübut; effektiv mübarizə

I. GİRİŞ

Cəmiyyətin idarə olunması, əsasən, zaman və məkan sərhədləri daxilində fəaliyyət göstərməsi üçün yaradılmış mexanizmlər vasitəsilə həyata keçirilmişdir. Kiberməkanda tənzimləmə isə məkan və zaman məhdudiyyətlərinin aradan qalxması ilə əlaqədar olaraq ənənəvi yanaşma və mexanizmlər vasitəsilə həyata keçirildikdə lazımi effekti vermir [1]. Bu hal analoji olaraq kiberməkanda törədilmiş cinayətlərlə mübarizə üsul və mexanizmlərinin effektivliyi və səmərəliliyinə də aid edilə bilər. Müasir cəmiyyətin və dövlətin davamlı inkişafını şərtləndirən İKT-nin geniş tətbiqinin limitsiz və azad informasiya axınını təmin etməsi bu imkanlardan cinayətkar məqsədlər üçün istifadə olunmasını istisna etmir. Rəqəmsal texnologiyaların yaratdığı mühit cinayətlərin törədilməsi və miqyasının genişlənməsi üçün münbit məkan rolunu oynayır.

Kiberməkan və fiziki məkan arasındakı kəmiyyət və keyfiyyət göstəricilərindəki fərqlər bu iki müxtəlif məkanda törədilmiş cinayətlərdə də öz əksini tapır. Kibercinayətkarlıqla mübarizənin effektivliyi və səmərəliliyinin təmin olunması bu fərqlərdən irəli gələn çətinlik və problemlərin ətraflı araşdırılması, onların həlli zamanı nəzərə alınması, həmçinin İKT-nin kibercinayətkarlıqla mübarizədə yaratdığı imkanların müəyyən olunması və tətbiqindən asılıdır. Belə ki, kiberməkan cinayətlərin törədilməsi üçün şərait yaratmaqla yanaşı, həm də onların araşdırılması və ya qarşısının alınması üçün yeni imkanları və çətinlikləri özündə birləşdirir.

II. KİBERCİNAYƏTKARLIĞIN MİQYASI

Cəmiyyətin və dövlətin həyatında və inkişafında İKT-dən geniş istifadə olunması ölkənin beynəlxalq müstəvidə rəqabət qabiliyyətini və davamlı inkişafını təmin etməklə yanaşı, ondan asılılığını da artırır. İKT-nin geniş tətbiqindən asılılıq isə öz növbəsində informasiya infrastrukturlarına edilən hər hansı hücum və müdaxilənin zərər vurma potensialını və həcmini yüksəldir. Son illərdə Azərbaycan Respublikasında e-hökumət, e-təhsil, e-səhiyyə, e-ticarət və s. sahələrə ayrılmış investisayalar sayəsində ölkənin informasiya infrastrukturunun əhəmiyyətli dərəcədə genişləndirilməsi, eyni zamanda, potensial kibercinayətkarlıq obyektlərinin də sayının artması kimi qəbul edilə bilər. İnformasiya infrastrukturuna edilmiş hücumlar, əsasən, kompüter sistemlərinin və ya məlumatlarının qəsdən zədələnməsi, silinməsi, korlanması, dəyişdirilməsi, bloklanması, saxtalaşdırılması, yaxud ələ keçirilməsi yolu ilə həyata keçirilir ki, bunlar da həm Kibercinayət haqqında Konvensiyaya, həm də Azərbaycan Respublikası Cinayət Məcəlləsinə əsasən kibercinayətkarlıq sayılan əməlləri təşkil edir [2][3].

Symantec Korporasiyası tərəfindən 2013-cü ildə hazırlanmış kibercinayətkarlıqla bağlı hesabatda dünya üzrə İnternetdən istifadə edən yetkin insanların 50%-nin kibercinayətkarlıqla və ya digər neqativ onlayn vəziyyətlərlə üzləşməsi ilə bağlı məlumatlar, ümumilikdə, kibercinayətkarlıqla mübarizə mexanizlərinin zəifliyinin göstəricisi kimi qəbul oluna bilər [4]. Hal-hazırda dünya əhalisinin 73%-nin (3 milyarrdan artıq), Azərbaycan Respublikası əhalisinin 73%-nin İnternetə çıxışla təmin olunması, İKT-nin inkişafı sahəsində qarşıya qoyulmuş məqsədə əsasən isə yaxın illərdə 85%-nin sürətli İnternetlə təmin olunacağını nəzərə alsaq, zəruri mexanizmlərin yerində olmamasının potensial zərərləri daha da aydın görünə bilər[5]. Həcmindən və hədəf obyektlərin sayından asılı olmayaraq yalnız bir və ya eyni anda bir neçə mənbədən, avtomatlaşdırılmış formada idarə oluna bilən, transmilli xarakterli kibercinayətkarlıqla mübarizə daha intensiv və adekvat mühafizə tədbirlərinin və mexanizmlərinin tətbiqini zəruriləşdirir. Buna görə də, informasiyalaşdırmaya yatırılmış invesitisiya ilə informasiya infrastrukturunun və vətəndaşların mühafizəsinə ayrılmış resurslar arasındakı mütənasibliyin asılılıqla risk arasındakı mütənasibliyə əsasən müəyyən olunması vacibdir. 2007-ci ilin aprel və may aylarında Estoniya Respublikasının bir sıra dövlət, media, bank və digər mühüm veb-saytlarının məruz qaldığı kiber hücumlar da məhz zəruri mühafizə tədbir və mexanizmlərinin çatışmazlığı səbəbindən əhəmiyyətli zərərlə nəticələnmişdi [6]. Həmin hücumların arxasındakı motiv bu gün Azərbaycan Respublikasının inkişafını istəməyən qüvvələr üçün də yad deyil. Üzvü olduğu Kibercinayətkarlıq haqqında Konvensiya və ya digər hüquqi mexanizmlərin Estoniya Respublikasına qarşı olan kiber hücumları istisna etməməsi, bunu deməyə əsas verir ki, Azərbaycan Respublikasının da kritik informasiya infrastrukturuna edilə biləcək cinayətkar motivli və ya düşmən xarakterli oxşar hücumlardan effektiv qorunması üçün həmin kritik informasiya infrastrukturlarının müvafiq mühafizə sistemləri ilə paralel təşkili və inkişaf etdirilməsi vacibdir.

III. KİBERCİNAYƏTKARLIĞIN ARAŞDIRILMASI

İKT-nin geniş istifadəsi və yaratdığı imkanlar həmçinin cinayət əməllərinin törədilməsindəki müxtəlifliklərlə müşayiət olunur. Bu texnologiyalardan istifadə etməklə törədilən

cinayətlərin qarşısının alınması üçün güclü mühafizə, cinayətlərin təhqiqatı və istintaqı üçün isə adekvat araşdırma alət və vasitələri tələb edilir. Araşdırma vasitələrinin adekvatlığı isə özündə həm texniki, həm də hüquqi cəhətləri birləşdirir. Kibercinayətkarlıqla effektiv mübarizə üçün cinayət hüququ ilə yanaşı, cinayət - prosessual hüquqi mexanizmlərin və müvafiq araşdırma texnikalarının inkişaf etdirilməsi zərurəti Kibercinayət haqqında Konvensiyanın izahedici məruzəsində də öz əksini tapmışdır [7].

Müasir dövrdə İKT-nin gündəlik həyatın bütün sferalarına daha dərindən təmas etməsi və insanlar tərəfindən daha geniş istifadə olunması, digər tərəfdən də, buraxılan elektron izlərin artmasına gətirib çıxarmışdır. Bu hal cinayətlərin törədilməsi zamanı buraxılan izlərə də aiddir. Buna görə də elektron sübutlar həm kibercinayətlərin, həm də İKT-dən istifadə etməklə törədilən digər cinayətlərin araşdırılması və müvafiq hökmün çıxarılması üçün əhəmiyyət daşıyır. Qeyd etmək lazımdır ki, elektron sübutlar cinayət işi başlama və ya işə başlamanı rəddetmə haqqında məsələnin həlli, ibtidai araşdırma zamanı hadisənin bütün mühüm hallarının tam, hərtərəfli və obyektiv araşdırılması, işdə mahiyyəti üzrə məhkəmə iclasında baxmaq üçün kifayətedici faktiki məlumatların və hüquqi əsasların olub-olmamasının yoxlanılması, daha sonra isə məhkəmə baxışı və hökmün çıxarılması mərhələsinin dəqiq və effektivliyinin əldə olunmasında həlledici rola malikdir. Bu mərhələlərin hər birinin prosessual qanunvericiliklə müəyyən olunmuş tələblərinə riayət olunması üçün elektron sübutların müəyyən olunması, əldə olunması, saxlanması, təhlili, məhkəmə baxışına təqdim edilməsi zəruridir. Bu isə hüquq mühafizə orqanlarından xüsusi texniki proqramlar, mexanizmlər, üsul və vasitələrin tətbiqini tələb edir. Bu tələblər İKT-nin istifadəsilə bağlı olduğuna görə hüquq mühafizə orqanlarının işinə bəzi aspektlərdən yardımçı olsa da, bir sıra hallarda çətinləşdirir.

A. İnformasiyanın həcmi və ötürülmə sürəti

Müasir kompüter yaddaşlarında saxlanılan və şəbəkələr vasitəsilə ötürülən böyük həcmdə informasiyanın araşdırılması məqsədilə seçilməsi və analiz olunması bu istiqamətdə əsas çətinliklərdən biridir[8]. Onu da qeyd etmək lazımdır ki, müasir texnologiyalar və kompüter sistemləri araşdırmanın sürətli və avtomatik həyata keçirilməsini təmin edə bildiyi üçün hüquq-mühafizə orqanlarına problemin texniki tərəfinin öhdəsindən nisbətən asanlıqla gəlmə imkanı yaradır [9]. Məsələn, beynəlxalq təcrübədə uşaq pornoqrafiyasının dövriyyəsi ilə bağlı cinayətlərin araşdırılması zamanı bu cür araşdırma proqramlarından geniş istifadə olunur. Lakin axtarışın avtomatlaşdırılması prosesi araşdırılan informasiyanın məzmun və formatından asılı olduğu üçün məhdud xarakter daşıyır və məzmunun qiymətləndirilməsi araşdırmanı yenidən həyata keçirən şəxslərin üzərinə düşür[10] .

Hüquq mühafizə orqanları üçün vəziyyəti mürəkkəbləşdirən digər bir cəhət ondan ibarətdir ki, cinayətin elementlərini özündə daşıyan informasiyanın ötürülməsi, əsasən, çox qısa bir zamanda - cəmi bir neçə saniyə ərzində həyata keçirilir. Bu isə araşdırma məqsədilə zəruri sübutların toplanılması üçün həddən artıq məhdud zamanın olması deməkdir. Eyni zamanda, elektron sübutların çox qısa bir zaman ərzində asanlıqla dəyişdirilə, tamamilə məhv edilə bilməsi cinayət təqibi üzrə icraat prosesində operativ və daha diqqətli davranmanı tələb edir. Bu çeviklik İKT-nin tətbiqilə əldə oluna bilən sayılsa da, mövcud normativ-hüquqi mexanizmlər adekvat çevikliyin əldə olunmasını hər bir halda təmin edə bilmir və ya etmir. Çünki müvafiq qanunvericilik sübutların toplanılmasında istifadə olunan üsul və vasitələrin seçilməsi və tətbiqində bir sıra müddəalara riayət olunmasını tələb edir. Məsələn, sübutların müəyyən olunması və toplanılması zamanı şəxsi məlumatların toxunulmazlığı ilə bağlı məhdudiyyətlər buna misal ola bilər [11, 12]. Qanunvericiliyin tələblərini pozmaqla aparılan prosessual hərəkətlərin prosessual qanunvericiliyə görə hüquqi qüvvəsinin olmaması bu kimi hallarda çevikliyi istər-istəməz ikinci plana keçirir [12]. Bundan başqa, maddi sübutların digər növlərindən fərqli olaraq, ən xırda diqqətsizliklə sübuti əhəmiyyətini tamamilə itirə biləcəyini nəzərə alaraq qeyd olunmalıdır ki, araşdırma zamanı əldə olunmuş elektron sübutların surətindən və ya şəklindən istifadə olunması onların orijinalının qorunması üçün, hər bir halda, daha məqsədəuyğundur [13]. Əlavə olaraq, qeyd etmək lazımdır ki, bulud texnologiyalarına (Cloud Computing) keçidin sürətlənməsi gələcəkdə kibercinayətlərin araşdırılması üçün zəruri olan elektron sübutların toplanması önündə əlyetərliliyin bir az da çətinləşməsi problemini yaradacaq və zəruri və mötəbər sübutların toplanmasını məhdudlaşdıracaq [14].

B. İnformasiyanın yeri, anonimlik və konfidensiallıq

İKT elektron sübutlarla bağlı çətinliklərin texnoloji tərəfinin həllində müəyyən rola və imkanlara malik olsa da, problemin hüquqi aspektlərinin həlli müvafiq normativ-hüquqi mexanizmlərin tətbiqindən asılıdır. Kibercinayətlərin təhqiqatı və istintaqı özündə adekvat araşdırma alət və vasitələrinin tətbiqi ilə yanaşı, elektron sübutlarla bağlı müvafiq prosessual qaydalara və qanunvericiliyə riayət olunmasını da tələb edir. Lakin sadəcə milli qanunvericiliyin təkmilləşdirilməsi kibercinayətkarlıqla mübarizənin effektivliyini və səmərəliliyini təmin etmir. Çünki cinayətin obyekti ilə subyekti arasındakı fiziki yaxınlığa və ya təmasa ehtiyac olmadan realizə olunan transmilli xarakterli kibercinayətlərin araşdırılması yurisdiksiya məsələləri ilə yanaşı, elektron sübutların da toplanmasında çətinlik yaradır [15]. Belə ki, bir sıra hallarda kibercinayəti törədən şəxsin yerinin müəyyən olunma prosesində yaranan çətinlik həmin cinayət üçün əhəmiyyət daşıyan elektron sübutların əldə olunması önündə də əngəllər yaradır. Eyni zamanda, infrastrukturun böyük hissəsinin özəl və ya şəxsi mülkiyyətdə olması hüquq - mühafizə orqanlarından müxtəlif sektorlarla əməkdaşlığı tələb edir [16].

Bu anlamda, daha bir diqqətəlayiq məqam isə kiberməkan üzərindən həyata keçirilən informasiya mübadilələrində anonimliyin və konfidensiallığın təmin olunması üçün imkanların geniş olmasıdır. Bu cür imkanların kibercinayətlərin realizəsi zamanı icraçılar tərəfindən geniş istifadə olunması cinayətlərin araşdırılması zamanı sübutların toplanması və qiymətləndirilməsi kimi hüquqi prosesləri mürəkkəbləşdirir. Qeyd olunduğu kimi, kiberməkan üzərindən törədilən bütün əməliyyatlar müəyyən izlər buraxır ki, bu da onların müvafiq metodlarla rahat izlənilə bilməsini mümkün edir. Onlayn əməliyyatlarda tam anonimliyin təmin olunmasının "mif" olduğunu nəzərə alsaq [17], kiberməkanın yaratdığı bu

maneənin də aşılmasının texnoloji həllinin çətin olmadığını anlamaq olar.

Bu, bütün hallarda araşdırma üçün lazımi informasiyaya limitsiz çıxışın əldə oluna bilməsi kimi qəbul edilməməlidir. Belə ki, informasiyanın yalnız sahibinə və ünvanlandığı şəxsə məlum olan alqoritmlərə əsasən şifrələnməsini həyata keçirərək daha yüksək səviyyəli konfidensiallıq təmin edən proqramların və texnologiyaların İnternet istifadəçiləri üçün əlyetərliliyi bu anlamda araşdırma qarşısında anonimlikdən daha böyük bir bir maneə yaradır. Açar şifrənin araşdırma orqanları tərəfindən şifrə sahibindən əldə edilə bilməsi məlumatların əlyetərliyinin mümkünsüzlüyünü aradan qaldırır. Lakin anonimliklə yanaşı, bu cür proqramlar vasitəsilə də şifrələnmiş bütün kommunikasiyalar və elektron sənədlər qanuni müdaxilələrə və axtarışlara qarşı immunitet qazanır, və bu cür həyata keçirilən elektron köçürmələr istənilən dövlət nəzarətindən kənarda qala bilir [16].

Kibercinayətlərin törədilməsində son illərdə bu metodlardan istifadə hallarının sürətlə artmasını nəzərə alaraq anonim və şifrələnmiş informasiya və sənədlərin sübut qismində toplanması, yoxlanılması, qiymətləndirilməsi, saxlanması ilə bağlı həm normativ-hüquqi, həm də elmi-texniki bazanın təkmilləşdirilməsi zəruridir.

C. Beynəlxalq müstəviyə çıxış

Müasir kompüter şəbəkələri vasitəsilə həyata keçirilən əməliyyatlarda ərazi yurisdiksiyaları üzrə fəaliyyət göstərən milli ənənəvi cinayət-hüquqi mexanizmlərinin təsir dairələrindən rahatlıqla kənara çıxıla bilməsi kibercinayətlərin törədilməsi üçün yeni imkanlar və hədəflər yaratmasına baxmayaraq, onların araşdırılması önünə bir sıra çətinliklər çıxarır. Çünki kiberməkan ərazilərə bölünərək yurisdiksiyalar üzrə fəaliyyət göstərmir və iş mexanizmi fiziki məkanda tətbiq olunan ərazi məhdudiyyətlərindən asılı deyil. Buna görə də, transmilli kibercinayətkarlığın araşdırılması və qarşısının alınmasında fiziki məkanın tələblərinə uyğunlaşdırılmış hüquqi mexanizmlər vasitəsilə effektivliyin təmini mümkün olmur. Kibercinayətkarlıqla hərtərəfli, səmərəli və effektiv şəkildə mübarizə aparılması və onların araşdırılması zamanı zəruri olan elektron informasiyanın toplanılması beynəlxalq əməkdaşlığı, xüsusilə də ölkələr arasındakı qarşılıqlı hüquqi və texniki yardımı şərtləndirir.

Beynəlxalq əməkdaşlıq və qarşılıqlı yardımın əldə olunması bir sıra formal hüquqi qaydalara riayət olunmasını şərtləndirdiyi, habelə əməkdaşlığın təşkili müəyyən zaman tələb etdiyi üçün kibercinayətin araşdırılması üçün zəruri olan operativliyin əldə olunması bir sıra hallarda mümkün olmur və nəticədə araşdırmanın səmərəsizliyinə gətirib çıxarır [14]. Araşdırmanın aparılması zamanı beynəlxalq əməkdaşlığın və yardımın əldə olunmasının sürətinin artırılması məqsədilə Kibercinayətkarlıq haqqında Konvensiyanın 35-ci maddəsində müəyyən olunmuş, sutkada iyirmi dörd saat, həftədə yeddi gün fəaliyyət göstərən müvafiq əlaqələndirmə mərkəzlərinin yaradılması nəzərdə tutulmuşdur [2].

NƏTİCƏ

İKT-nin müasir həyatın və inkişafın bütün sferalarını geniş şəkildə əhatə etməsi, qlobal məkana və informasiyaya çıxışdakı sərhədləri aradan qaldırması, informasiya mübadilələrinin və əməliyyatların yüksək sürətini təmin etməklə yanaşı, ucuzluğu və əlyetərliliyi qısa bir zaman ərzində dünya əhalisinin təxminən yarısının istifadəçiyə çevrilməsi ilə nəticələnmişdir. Bütün bunlar isə kibercinayətlərin araşdırılmasının həyata keçirilməsi üçün yeni üsul və vasitələrlə yanaşı, onların realizəsində yeni metod və imkanların yaranmasına, habelə potensial kibercinayətkarlıq obyektlərinin sayının və miqyasının sürətlə artmasına gətirib cıxarmışdır. Kiberməkanın səciyyəvi xüsusiyətləri, habelə infrastrukturun, əsasən, özəl sektor və vətəndaşların əlində cəmlənməsi kibercinayətkarlıqla mübarizədə adekvat institutsional strukturların, elmi-texniki və normativ-hüquqi bazanın formalaşdırılması və təkmilləşdirilməsi ilə yanaşı, dövlət, özəl sektor və vətəndaşlar arasında, həmçinin beynəlxalq səviyyədə tərəfdaşlığın və əməkdaşlığın genişləndirilməsini tələb edir. Adekvat mexanizmlərin, zəruri institutların, çoxtərəfli və beynəlxalq tərəfdaşlıq və əməkdaşlığın yerində olmaması isə kibercinayətkarlıqla mübarizəni daha da müəkkəbləşdirir və çətinləşdirir.

ƏDƏBİYYAT

[1] Y. Akdeniz, C. Walker, D.Wall, The Internet, Law and Society. Longman, 2000.

[2] Convention on Cybercrime, Council of Europe, Budapest, 23 November 2001 (ETS No. 185). http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[3] Azərbaycan Respublikasının Cinayət Məcəlləsi, (maddə 271 - 273-2).

[4] Symantec Corporation, Norton Cybercrime Report 2013. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

[5] http://www.internetworldstats.com/asia.htm

[6] Estonia under cyber attack, Compiled by Beatrix Toth (Hun-CERT), http://cert.hu/sites/default/files/Estonia_attack2.pdf

[7] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

[8] M. Yar, Cybercrime And Society. (SAGE Publications 2013, 2nd edn)

[9] T.J. Holt, A.M. Bossler, K. C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction , Routledge 2015.

[10] IWF, Content Assessment Appeal Process, https://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process

[11] Azərbaycan Respublikasının Konstitutsiyası, (maddə 32).

[12] Azərbaycan Respublikasının Cinayət Prosessual Məcəlləsi, (maddə 10; 16).

[13] B.Shavers and H.Carvey, Placing The Suspect Behind The Keyboard. Syngress, 2013.

[14] The ITU publication, Understanding cybercrime: Phenomena, challenges and legal response. 2014 Available online at: www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf

[15] M. Mueller, Networks and States. MIT Press, 2010.

[16] C. Jonathan, Principles of cybercrime. Cambridge University Press, 2010.

[17] D. Wall, Policing Cybercrimes: Situating The Public Police In Networks of Security Within Cyberspace. 2007.