Milli kibertəhlükəsizlik və internet azadlığı

Bəxtiyar Məmmədov[1], Aysel Əsgərova[2]

Azərbaycan Respublikası Rabitə və Yüksək Texnologiyalar Nazirliyi
[1]law@mincom.gov.az, [2]law-aysel@mincom.gov.az

***Xülasə*— İnternet hər birimizin həyatının ayrılmaz tərkib hissəsinə çevrilmişdir. Lakin bu daimi bağlılıq oğurluq, dələduzluq və sui-istifadə risklərini də artırır. Heç bir dövlət, sənaye sahəsi, icma və ya fərd kiber risklərdən sığortalanmamışdır. Kibertəhlükələr fərdlərin maliyyə, identifikasiya və şəxsi həyat toxunulmazlığına yönəldiyi halda, dövlətlər müntəzəm olaraq öz kritik infrastrukturlarına və iqtisadiyyatına yönəlmiş kiber təhdidlərlə üzləşirlər. İnsanların həyatı kritik infrastrukturlardan və onları idarə edən rəqəmsal texnologiyalardan asılı olduğu üçün dövlətin kibertəhlükəsizliyi milli təhlükəsizliyin ən mühüm prioritetlərindən biri hesab edilə bilər. Lakin milli təhlükəsizlik əleyhinə yönəlmiş kibertəhdidlərlə mübarizə fərdlərin şəxsi toxunulmazlıq və azadlığının və ya texnologiyanın inkişafı üçün zəruri olan innvovasiyanın qarşısını almamalıdır. Məqsədlərdən asılı olmadan internetdə həyata keçirilən texniki tədbirlər proporsionallıq, qanunun aliliyi, şəffaflıq prinsipləri üzərində qurulmalıdır. Bu araşdırmada milli təhlükəsizlik əleyhinə yönəlmiş kibertəhdidlərlə mübarizə zamanı fərdlərin onlayn hüquq və azadlıqlarının həyata keçirilməsi məsələləri təhlil olunur.**

Açar sözlər— milli kibertəhlükəsizlik; kritik infrastrukturlar; internet azadlığı.

I. GİRİŞ

Müasir "milli təhlükəsizlik" konsepsiyası və elektron rəqəmsal kompüterin meydana gəlməsi II Dünya müharibəsinin məhsulu olaraq təxminən eyni vaxta təsadüf etmişdir [1]. Yaxın keçmişə qədər milli təhlükəsizlik konsepsiyası ilə qarşılıqlı faydalı münasibətdə mövcud olmuş kompüter texnologiyası bu gün də milli təhlükəsizlik üçün mühüm əhəmiyyət daşıyır. Lakin, internetin və şəbəkə kompüterlərinin dövlətlərin təhlükəsizliyi üçün yaratdığı çətinliklər dövlətlərin narahatlığına səbəb olmuşdur.

İnternetin, xüsusilə sosial şəbəkələrin təsiri biznes və siyasətlə məhdudlaşmır, qaçılmaz şəkildə milli təhlükəsizliyi də hədəfə alır. Xüsusilə sosial şəbəkələr milli təhlükəsizliyin hər bir aspektinə, o cümlədən açıq mənbələrdə ictimaiyyət üçün açıq olan informasiyanın toplanması və araşdırılması, ictimai rəyin ölçülməsi və ona təsir edilməsi, tədqiqat və analiz aparılması, sahə üzrə siyasət, proqramların və fəaliyyət növlərinin planlaşdırılması və tətbiqi, informasiya əməliyyatlarının həyata keçirilməsinə (kompüter şəbəkə əməliyyatları, psixoloji əməliyyatlar, ictimai fikrin çaşdırılması, əməliyyat təhlükəsizliyi və s.) təsir göstərmək potensialına malikdir.

Karafanoya görə təşkilatda ən yaxşı informasiyanın effektiv şəkildə təmizlənməsi və paylaşdırılması üçün iki model mövcuddur: yuxarıdan aşağıya doğru və aşağıdan yuxarıya doğru [2]. Birinci modeldə təşkilatdakı yüksək vəzifəli işçilər ən yaxşı informasiyanı toplayır və onun formalaşdırılması, redaktə olunması, biliyə çevrilməsi və bundan sonra yayılması üçün öz təcrübə və bacarıqlarından istifadə edirlər. Bu biliyin yaradılmasının və idarə edilməsinin iyerarxik modeli yüksək vəzifəli işçilər üçün tanış olan sabit və proqnozlaşdırıla bilən mühitdə daha effektiv işləyir. Lakin təcrübənin köməksiz olduğu dinamik vəziyyətlərdə, o cümlədən onlayn mühitdə biliyin yaradılması ikinci model, yəni aşağıdan yuxarıya doğru işləyir. Adi sosial şəbəkə ünsiyyəti zamanı informasiyanı qiymətləndirərkən "kütləyə etibar etmək" metodu münasib olsa da, milli təhlükəsizliyə, insanların həyatı və ya dövlət xəzinəsi ilə bağlı məsələlərə toxunan məsələlərdə bu metodun yararlı olması böyük şübhə doğurur.

İnformasiya texnologiyaları fərdlərə daha çox və daha yaxşı analiz həyata keçirmək imkanı verir, lakin o həm də ictimai rəy formalaşdıran fərdlərə provokativ xarakterli mövzuları daha sürətlə və daha geniş kütlə arasında yaymağa kömək edir. Bu gün bütün dünyada ekstremist baxışların genişlənməsinin ən mühüm səbəbi radikal materialların internetdə asanlıqla əldə edilə bilməsidir. İnformasiya texnologiyalarının imkanları sayəsində insanları qorumaq üçün toplanmış məlumat çox qısa müddət ərzində onlara qarşı istifadə edilə bilər və ya heç kim tərəfindən görülməməli informasiya dəqiqələr içində hamıya aşkar ola bilər. Məhz bu səbəbdən milli təhlükəsizliyə aid olan məsələlərdə informasiyaya təminat verilməsində onlayn kütləyə etibar edilməsi yolverilməz görünür. Bununla yanaşı, milli təhlükəsizlik əleyhinə yönəlmiş kibertəhdidlərlə mübarizə fərdlərin şəxsi toxunulmazlıq və azadlığın və ya texnologiyanın inkişafı üçün zəruri olan innvovasiyanın qarşısını almamalıdır.

II. AZAD İNTERNET VƏ ONLAYN İFADƏ AZADLIĞI HÜQUQU

İnternet insanların öz fundamental hüquq və azadlıqlarını tətbiq və istifadə etdikləri bir məkana çevrilmişdir. Burada onlar şəxsi və işgüzar həyat fəaliyyətlərini həyata keçirir, eləcə də ictimai həyat və demokratik söhbətlərdə iştirak edirlər. Bu gün dünyada 3 milyard internet istifadəçisi var [3].

İnternetin həyatımızı tamamilə dəyişdirməsinə baxmayaraq, insanların internetə məhdudiyyətsiz daxil olmaq, onlayn alış-veriş etmək, sosial mediadan istifadə etmək qabiliyyətinə təminat verilmədən və informasiya axınının təhlükəsiz olmasına zəmanət vermədən bu cür dəyişikliyin davamlı olaraq müsbət məcrada davam edəcəyinə inanmaq çətindir. Bu baxımdan təhlükəsizlik azadlığın vacib şərtidir. Azadlıq və vətəndaşların fəal iştirakı isə təhlükəsizlik üçün vacib amillərdir. Avtoritar rejimlər cəmiyyətin azadlığı ilə onun təhlükəsizliyini tərs mütənasib göstərməyə çalışsa da, bu cür ölkələrdə fərdi azadlıqlar həyatın bütün sahələrində, o cümlədən internetdən istifadə sahəsində kobud şəkildə pozulur. Beləliklə, təhlükəsizlik azadlığın, azadlıq isə təhlükəsizliyin vacib şərtidir və onlardan birinin digərinin xeyrinə məhdudlaşdırılması tarazlığın pozulmasına səbəb ola bilir [4].

Açıq, azad və təhlükəsiz internetin təmin edilməsi də əsas çətinliklərdəndir. Belə ki, vətəndaşlar və bizneslər öz informasiya və pullarını itirmədən internetin təklif etdiyi bütün üstünlüklərdən yararlana biləcəklərindən əmin olmalıdırlar. Bu gün kibercinayət istər bank sistemlərinə massiv hücumlar, istərsə də uşaqların istismarı şəklində mütəşəkkil cinayətkar dəstələr üçün ən cəlbedici gəlir mənbələrindən birinə çevrilmişdir. Lakin yalnız mütəşəkkil cinayətkar dəstələr deyil, dövlət və qeyri-dövlət subyektləri də internetdən həssas informasiyanın izlənilməsindən kritik infrastruktura zərər vurulmasına qədər dağıdıcı məqsədlərlə istifadə edilməsi qabiliyyətini qısa müddət ərzində mənimsəmişlər. (Məhv edilməsi və ya parçalanması milli və ya regional fəlakətə səbəb ola biləcək istənilən sistem və ya resurs kritik infrastrukturun bir hissəsi hesab edilə bilər. Bura dövlətə və özəl sektora aid olan banklar, elektrik stansiyaları, telefon şirkətləri, internet xidmət provayderləri və s. aid edilə bilər.)

Terrorizmin qarşısının alınması və kibertəhlükəsizliyin möhkəmləndirilməsi ictimai problemlər olduğu üçün onların həlli də cəmiyyətin iştirakını zəruri edir. Təhlükəsizliyi təmin edən hüquq mühafizə orqanları kimi ənənəvi qurumlar hələ də vacibdir, lakin onlar öz vəzifələrinin öhdəsindən tək gələ bilməzlər. Məsələn, gənc insanların Suriyaya getməsini həvəsləndirməyin qarşısını almaqda polis köməksiz görünür. Bəzi müəlliflər problemin həllini iştirakçılar dairəsinin hüquq mühafizə orqanları, vətəndaş cəmiyyəti, özəl sektor, terrorizm qurbanları, akademiya və digərləri hesabına genişləndirməyi çıxış yolu kimi göstərirlər [5].

İnternet azadlığı mədəni və siyasi fərqliliklərlə məhdudlaşdırılmadan vəhdət şəklində təfsir olunmalıdır. Bu tədqiqatın məqsədləri üçün internet azadlığı şəxsi həyat və ifadə azadlığı hüququ, eləcə də media və toplaşmaq azadlığı ilə bağlı internetdən istifadəni nəzərdə tutur.

Yeni texnologiyaların, aplikasiya və xidmətlərin davamlı inkişafı hüquq və azadlıqların müdafiəsi üçün bir sıra çətinliklər yaratmaqdadır. Bu texnologiya, aplikasiya və xidmətlərin nəzarət və müşahidə etmək, məzmuna daxil olmanı idarə etmək və məzmuna daxil olmanın qarşısını almaq qabiliyyətinə malik olması hazırda ən böyük problemlərdəndir.

Dövlətlər internetlə əlaqədar fundamental hüquq və azadlıqlara hörmət edilməsi, onların qorunması və təşviq edilməsi və internet azadlığı üçün əlverişli mühit yaradılmasında məsuliyyət daşıyırlar. Bu sahədə dövlətlərin fəaliyyəti internet azadlığının mövcudluğu və inkişafı üçün zəruri olan hüquqi, iqtisadi və siyasi şərtlərin dəyərləndirilməsi məqsədilə milli səviyyədə internet azadlığı mühitinin müntəzəm şəkildə qiymətləndirilməsini özündə ehtiva etməlidir. Bu cür qiymətləndirmələr internetlə əlaqədar insan hüquq və azadlıqlarının pozulmasının qarşısının alınmasına, mövcud standartların daha yaxşı tətbiqinə, dövlət idarəetməsinin keyfiyyətinin artırılmasına və internetlə əlaqədar milli strategiyaların inkişafına töhvə verir.

III. İFADƏ AZADLIĞI HÜQUQU

İnternetdə ifadə azadlığı sərhədlərdən asılı olmayaraq tətbiq olunur. Dövlətlər bu hüquqa tətbiq edilmiş istənilən məhdudiyyətin digər dövlətlərin vətəndaşlarına təsir etməməsinə təminat vermək vəzifəsi daşıyırlar. Vəzifə və məsuliyyət nəzərdə tutduğu üçün ifadə azadlığı məhdudlaşdırıla bilər. İnternetdə ifadə azadlığına məhdudiyyət nəzərdə tutan qanunlar əldə edilə bilən, aydın, birmənalı və fərdlərə öz əməllərinin qanuni olmasını əvvəlcədən görə bilmələri üçün kifayət qədər dəqiq olmalıdır.

Bu cür məhdudiyyətləri nəzərdə tutan qanunlar və siyasət məhdudiyyətlərin tətbiqi məqsədi ilə ifadə azadlığını qorumaq vəzifəsi arasında tarazlığın qorunmasına təminat verməlidir. Məhdudiyyətlər qanuni məqsəd daşımalı, zəruri və proporsional olmalıdır.

Qanunlar internetdə ifadə azadlığına görə cinayət məsuliyyəti nəzərdə tutmamalıdır. Nifrət aşılayan nitqlər, terrorizm əleyhinə tədbirlər kimi spesifik məsələləri tənzimləyən və cinayət məsuliyyəti nəzərdə tutan qanunlar spesifikdir və yalnız tənzimləməli olduqları məsələlərə yönəlirlər.

IV. QOŞULMAQ AZADLIĞI

İnternetdə ifadə azadlığı giriş vasitəsi, məzmun və ya istifadə edilən xidmətdən asılı olmadan tətbiq edilir. İnfrastruktur ifadə azadlığı hüququnun mümkün edən amildir. Bütün vətəndaşların internetə çıxışı imkanını təmin etmək məqsədilə dövlət internetin bütün əhali qrupları üçün əldə edilə bilən olmasını təmin edən infrastruktur siyasəti həyata keçirir.

Dövlət həmçinin internetin azlıqlar və həssas qruplar da daxil olmaqla hər hansı qrup üçün ayrı-seçkilik olmadan əldə edilə bilən olmasını təmin etmək üçün tədbirlər həyata keçirməlidir.

Dövlət internetə girişə müdaxilə etmir. Dövlət siyasəti və qanunvericilik internetə girişin bütün infrastruktur növlərinin provayderləri tərəfindən bütün vaxtlarda (siyasi qeyri-sabitlik, gərginlik və s.-dən asılı olmadan) təmin edilməsini tələb etməlidir.

Şəxsi həyat və internetdə ifadə azadlığının pozulması hesabına olsa belə daxildən və xaricdən gələn təhlükə riskləri ilə üzləşən, sülh və ictimai asayişi qorumaq kimi qanuni məqsədlərlə milli təhlükəsizliyi qorumaq istəyən dövlətlər mövcuddur. Məqsədlərdən asılı olmadan internetdə həyata keçirilən texniki tədbirlər proporsionallıq, qanunun aliliyi şəffaflıq prinsipləri üzərində qurulmalıdır. Bu sahədə beynəlxalq və regional təşkilatlar tərəfindən üzv-ölkələr üçün tövsiyə xarakterli sənədlər və standartlar işlənib hazırlanır. 2015-ci il 1 aprel tarixində Avropa Şurası Nazirlər Komitəsinin 1224-cü iclasında təşkilatın Rabitə və Yüksək Texnologiyalar Nazirliyinin də təmsil olunduğu Ekspertlər Komitəsinin əvvəlki iclaslarında təkmilləşdirilmiş“ Trans-sərhəd internet axını və internet azadlığı üzrə tövsiyələr” qəbul edilmişdir. Sənəddə internetdə informasiyanın maneəsiz transsərhəd axını ifadə, toplaşmaq, qoşulmaq azadlığı kimi hüquqların tam həyata keçirilməsi, mədəni, təhsil, innovasiya və iqtisadi inkişafın əsas amili kimi göstərilir, maneəsiz transsərhəd axınının əsas prinsipləri, tənzimləmə, yaxşı təcrübələrin təşviqi, beynəlxalq dialoq və siyasət məsələləri əks olunur [6].

NƏTİCƏ

İnsanların həyatı kritik infrastrukturlardan və onları idarə edən rəqəmsal texnologiyalardan asılı olduğu üçün dövlətin kibertəhlükəsizliyi milli təhlükəsizliyin ən mühüm prioritetlərindən biri hesab edilir. Lakin milli təhlükəsizlik

əleyhinə yönəlmiş kibertəhdidlərlə mübarizə fərdlərin şəxsi toxunulmazlıq və azadlığının və ya texnologiyanın inkişafı üçün zəruri olan innvovasiyanın qarşısını almamalıdır.

Milli təhlükəsizliyi qoruyarkən dövlət onlayn dünyada ifadə azadlığının vacibliyini, şəffaflıq prinsipini nəzərə almalı, məsələnin yalnız hakimiyyət səlahiyyətləri ilə deyil, sənayenin iştirakı və onunla əməkdaşlıq vasitəsilə həll edilməsinə üstünlük verməlidir. Həmçinin dövlətin kibertəhlükəsizliyinin onun vətəndaşlarının birgə məsuliyyəti məsələsi olması da nəzərə alınmalıdır [7].

İstənilən halda məqsədlərdən asılı olmadan, internetdə həyata keçirilən texniki tədbirlər proporsionallıq, qanunun aliliyi, şəffaflıq prinsipləri üzərində qurulmalıdır.

ƏDƏBİYYAT

[1] G. Chapman, “National Security and the Internet”July 2014, http://www.utexas.edu/lbj/21cp/isoc.htm

[2] J.J.Carafano, “Understanding Social Networking and National Security” Joint Force Quarterly; 2011 1st Quarter, Issue 60, p73

[3] International Telecommunications Union, “The World in 2014: ICT Facts and Figures”

[4] C. Malmström, “Rebooting Trust? Freedom vs. Security in Cyberspace” 31 January 2014 http://europa.eu/rapid/press-release_SPEECH-14-87_en.htm

[5] C. Malmström, “Rebooting Trust? Freedom vs. Security in Cyberspace” 31 January 2014. http://europa.eu/rapid/press-release_SPEECH-14-87_en.htm

[6] Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet

[7] Freedom of Expression and Democracyin the DigitalAge. Opportunities, Rights, Responsibilities. (Belgrade, 7-8 November 2013) CoEConference of Ministers, Political Declaration and Resolutions.