# İnformasiya təhlükəsizliyi sahəsində beynəlxalq çağırışlar, təşəbbüslər və öhdəliklər

Vüqar Musayev[1], Yadigar İmamverdiyev[2]

*AMEA İnformasiya Texnologiyaları İnstitutu*

[1]iro@iit.ab.az, [2]yadigar@lan.ab.az

***Xülasə*— Məqalədə informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlıqla bağlı qlobal təşkilatların və regional qurumların təşəbbüsləri və konkret fəaliyyət istiqamətləri araşdırılmışdır. Bu sahədə siyasi, hüquqi, elmi-texniki müstəvidə, həmçinin xüsusi istiqamətlər üzrə beynəlxalq təşkilatların əsas fəaliyyət istiqamətləri və qarşılıqlı əlaqələri xülasə olunmuşdur.**

***Açar sözlər*— *informasiya təhlükəsizliyi, kibertəhlükə, kibercinayət, IMPACT, ENISA, FIRST, INSAFE***

## I. GİRİŞ

İnformasiya və kommunikasiya texnologiyaları (IKT) hər gün həyatımıza daha geniş daxil olur: məişətdə, işdə, təhsildə, səhiyyədə, ticarətdə istifadə edilir, dövlət orqanları ilə qarşılıqlı əlaqəni asanlaşdırır. Qısaca, biz "virtual reallıq" dövründə yaşayırıq.

Lakin real həyatda mövcud olan mənfi elementlər: dələduzluq, cinayətkarlıq, zorakılıq halları virtual dünya proyeksiyalanır və spamlar, viruslar, fərdi məlumatların ələ keçirilməsi, şantaj, pornoqrafiya, kibercinayətkarlıq, kiberterrorizm kimi bütün dünyanın birgə mübarizə aparmaqla minimallaşdırılması mümkün olan təhdidlər yaranır.

Kiberfəzada sərhədlər və məhdudiyyətlər yoxdur, kibertəhdidlər istənilən yerdə baş verə və qısa müddət ərzində böyük ziyan vura bilərlər. Buna görə də IKT-nin istifadəsi zamanı inamın və təhlükəsizliyin yüksəldilməsi dünya ictimaiyyəti üçün ən aktual məsələlərdən birinə çevrilir.

Kiberfəzada hücumçular hədəfdən çox uzaq məsafədə, bir çox halda bu sahədə qanunvericiliyi çox zəif olan ölkələrdən edilə bilər. Sürətli kommunikasiya imkanları hücuma məruz qalan tərəfin özünü müdafiə üçün çox az vaxt tələb olunur. Yaxşı halda, dövlətlət və təşkilatlar hücuma məruz qaldıqlarını anlayır, ən pis halda isə kritik sistemlərinin ələ keçirildiyini belə bilmir [1].

Yuxarıda qeyd olunan məsələlərdən aydın olur ki, ölkələrin kibercinayətkarlıqla fərdi şəkildə mübarizələri ilə yanaşı beynəlxalq əməkdaşlıq qaçılmazıdr. Beynəlxalq təşkilatların və informasiya təhlükəsizliyi ilə bağlı qurumların bu sahədə apardığı beynəlxalq əməkdaşlığın mövcud vəziyyətinin araşdırılması və təcrübənin öyrənilməsi bu baxımdan aktualdır.

## II. İNFORMASİYA MÜHARİBƏSİ TƏHLÜKƏSİ

Beynəlxalq informasiya təhlükəsizliyinin təmin edilməsi problemlərinə baxıldıqda bir-biri ilə qarşılıqlı əlaqəli hərbi-siyasi, kriminal və terror xarakterli üç növ təhdidin olmasından çıxış etmək lazımdır. İKT-ni təkcə hər hansı qanun pozucusu, cinayətkar qruplar, terrorçu və ekstremist təşkilatlar deyil, dövlətlər də düşmən siyasi, iqtisadi və hərbi məqsədlərlə istifadə edə bilərlər. Bu yolla örtülü təcavüz həyata keçirərək milli, regional və qlobal səviyyədə təhlükəsizlik təhdidləri yaradırlar.

Bəzən informasiya silahını kütləvi qırğın silahları, o cümlədən nüvə silahları ilə müqayisə edirlər və dağıdıcılığına görə üstünlüyü informasiya silahlarına verirlər. Məlumatlara görə dünyanın 120 ölkəsi informasiya sılahının işlənilməsi sahəsində fəaliyyətlə məşğuldur. Nüvə silahının yaradılması sahəsində isə on beşə yaxın ölkənin çalışdığı məlumdur. Stuxnet, Duqu, Gauss, Flame kimi viruslar bu silahların gerçək gücünü nümayiş etdirmişdir [2]

## III. BEYNƏLXALQ ƏMƏKDAŞLIQ

İnformasiya təhlükəsizliyinin təmin edilməsində beynəlxalq əməkdaşlıq həyati əhəmiyyət daşıyır, çünki hamı bir kiberfəzadan asılıdır və bir ölkədə olan kibertəhlükəsizlik boşluqları digər ölkələrə təsir edə bilər. Lakin bu strateji sahədə xarici ölkələrlə əməkdaşlıqda iqtisadi, siyasi, və milli təhlükəsizlik risqləri də mövcuddur. Beynəlxalq əməkdaşlıq qanunvericilik tədbirləri, kibercinayətkarlıqla mübarizə, insidentlərin cavablandırılması, elmi-tədqiqatlar, aparat və proqram təminatının sertifikatlaşdırılması kimi sahələri əhatə edə bilər [3].

İnformasiya təhlükəsizliyi sahəsində ilkin beynəlxlq əməkdaşlıq G8 zirvəsinin "Yüksək Texnologiyalarla bağlı Cinayətlər" üzrə alt komitələrində başlamışdır. 1997-ci ildə G8 zirvəsində INTERPOL təşkilatı ilə birlikdə "24/7 Network of Contacts" proqramı yaradılmışdır [4,5]. Bu proqramın məqsədi dövlətlərə terrorçuların kommunikaslya mənbələrinin aşkarlanması, təhdidlərin araşdırılması və gələcək hücumların qarşısının alınması məsələlərində kömək etmək idi.

Burada iştirakçı dövlətlər kibercinayətlərlə bağlı informasiya mübadiləsi və rəsmi kontakt nöqtəsinin təyin edilməsini öhdəliyinə götürürdü.

Oxşar təçəbbüs FBI tərəfindən irəli ürülmüş və İnternet Cinayətləri Şikayət Mərkəzi (Internet Crime Complaint Center-IC3) qurulmuşdu. 2007-ci ildə 47 ölkə bu şəbəkəyə qoşulmuşdu [6].

İnformasiya təhlükəsizliyinin qlobal miqyasda təmin edilməsi problemi ilk dəfə 2002-ci ildə G8 ölkələrinin liderlərinin qəbul etdiyi "Qlobal informasiya cəmiyyətinin Okinava xartiyası"nda qabardılmışdı [7]. Sonrakı mərhələ informasiya cəmiyyəti məsələləri üzrə ümumdünya sammitləri oldu. Ümumdünya sammitlərinin yekun sənədlərində İKT-nin

qlobal, regional və milli səviyyələrdə istifadəsi zamanı təhlükəsizliyin təmin edilməsi üzrə real tədbirlərin görülməsinin zəruriliyi əks olunmuşdur.

İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (OECD: Organisation for Economic Co-operation and Development) 2002-ci ildən bəri informasiya təhlükəsizliyi sahəsində aktiv iştirak edir. OECD-nin müvafiq qurumu WPISP (Working Party on Information Security and Privacy) [8] ildə 2 dəfə Parisdə toplanır və informasiya sistemləri və şəbəkələrinin təhlükəsizliyi ilə bağlı bir sıra sənədlər nəşr edir. Bu sənədlərə aşağıdakı nümunələri göstərmək olar:

- "Guidelines for the Security of Information Systems and Networks" (2002);
- "Promotion of a Culture of Security for Information Systems and Networks" (2005).

## IV. BEYNƏLXALQ TELEKOMMUNİKASİYA İTTİFAQININ KİBERTƏHLÜKƏSİZLİK TƏŞƏBBÜSLƏRİ

Ümumdünya sammitlərinin qərarlarının informasiya təhlükəsizliyinin təmin edilməsi sahəsində həyata keçirilməsi "İKT-nin istifadəsi zamanı inam və təhlükəsizliyin möhkəmləndirilməsi" fəaliyyət istiqaməti çərçivəsində reallaşdırılır. Bu prosesdə Beynəlxalq Telekommunikasiya İttifaqına (BTİ) böyük rol ayrılıb. Bu sahədə BTİ-nin fəaliyyət istiqamətləri BMT-nin müvafiq qətnamələri, BTİ-nin səlahiyyətli konfranslarının qərarları Qlobal Kibertəhlükəsizlik Proqramı, elektrorabitənin inkişafı üzrə fəaliyyət planı (Haydarabad, 2010) və BTİ-nin digər sənədləri ilə müəyyən edilir.

"Kibertəhdidləri fəal şəkildə izləmək və qarşısını almaq üçün" 2009-cu ildə BTİ tərəfindən International Multilateral Partnership Against Cyber Threats (IMPACT) proqramı işə salınmışdır [9].

IMPACT BMT-nin dəstəklədiyi ilk kibertəhlükəsizlik alyansıdır. Neytral siyasi platforma kimi IMPACT 152 ölkəni özündə birləşdirir. Baş qərargahı Malayziyada yerləşən IMPACT BTİ-yə üzv-ölkələrə xidmət etməklə yanaşı, BMT-nin qurumlarının İKT infrastruktutunun informasiya təhlükəsizliyinə dəstək verir. Bu təşkilat kibertəhdidlərin aşkarlanması, analizi və qarşısının effektiv alınması sahəsində üzv-ölkələrə ekspert xidmətləri və zəruri resurslar təqdim edən ilk beynəlxalq əməkdaşlıq təşkilatıdır.

ITU-IMPACT birliyinin üzv ölkələri aşağıdakı imkanlardan yararlana bilərlər:

- IMPACT təşkilatına məxsus qlobal informasiya təhdidlərinə nəzarət mərkəzinin resurslarına pulsuz giriş.
- "Ekspertlər üçün təhlükəsiz elektron əməkdaşlıq platforması" (Electronically Secure Collaboration Application Platform for Experts – ESCAPE) birliyinə aid resurslara pulsuz giriş. Bu platforma müxtəlif ölkələrin ekspertlərinə kibertəhlükəsizlik sahəsində bilik və təcrübələrini bölüşdürməyə, kiberhücumlardan müdafiə zamanı yardım göstərilməsinə imkan verir.
- ITU-IMPACT üzv ölkələrin milli CERT komandaların kommunikasiya və insidentləri cavablandırma imkanlarının yüksəldilməsi üzrə kiber təlimlər və seminarlar təşkil edir (Applied Learning for Emergency Response ,Teams, ALERT).

## V. AVROPA ŞƏBƏKƏ VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ AGENTLİYİNİN FƏALİYYƏTİ

Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyinin (European Network and Information Security Agency, ENISA) məqsədi şəbəkə və informasiya təhlükəsizliyi sahəsində mədəniyyətin formalaşdırılması yolu ilə Avropa İttifaqında şəbəkə və informasiya təhlükəsizliyinin yüksəldilməsidir. ENISA 2004-cü ilin yanvarında Nazirlər Şurası və Avropa Parlamenti tərəfindən "yüksək texnologiya" cinayətlərinə cavab vermək üçün yaradılmışdı. Agentlik aşağıdakı vəzifələri yerinə yetirir [10]:

- ENISA və Avropa İttifaqı üzvləri arasında şəbəkə və informasiya təhlükəsizliyinin təmin edilməsi məqsədi ilə dəstək göstərilməsi;
- Maraqlı tərəflər arasında davamlı informasiya mübadiləsinə kömək göstərilməsi;
- Şəbəkə və informasiya təhlükəsizliyi ilə əlaqəli olan funksiyaların koordinasiyasının yaxşılaşdırılması.

## VI. BEYNƏLXALQ QANUNVERİCİLİK

Avropa Şurasının Kibercinayətkarlıq üzrə Konvensiyası (Budapeşt konvensiyası) [11], xüsusilə onun 32-ci maddəsi (trans-sərhəd girişi haqqında) bir sıra tənqidlərə məruz qalır. Bu maddə digər ölkənin xüsusi xidməti orqanlarına başqa ölkənin dövlət orqanlarının razılığı olmadan həmin ölkənin kompüter şəbəkələrinə daxil olaraq orada əməliyyatlar aparmağa imkan verir. Bu müddəa dövlət suverenliyini pozur və bir sıra ölkələrin bu maddənin Konvensiyadan çıxarılması və ya redaktə edilməsi tələbləri sənədi imzalayan ölkələr tərəfindən dəstəklənmir.

Qanunvericilikdə daha bir məsələ informasiyanın və IKT-nin qanunsuz istifadəsi ilə bağlı məsələlərin yalnız kibertəhdidlər ilə məhdudlaşdırılmasıdır. ABŞ-ın yanaşmasında, informasiya-psixoloji əməliyyatlara beynəlxalq-hüquq nizamlanması sahəsində baxılmır, belə əməliyyatlar son dövrlər IKT vasisəsilə, xüsusi halda sosial şəbəkələr vasitəsilə tez-tez həyata keçirilir. Bu məsələlərin informasiya təhlükəsizliyi sahəsinə aid edilməsi cəhdləri "vətəndaş cəmiyyətinə təzyiq", "söz azadlığına təhdid", "avtoritar tendensiyaların gücləndirilməsi" cəhdləri kimi qiymətləndirilir.

Kibertəhlükəsizlik sahəsində milli qanunvericiliyin beynəlxalq standartlara uyğunlaşdırılması da ölkələr qarşısında duran vacib məsələdir.

Avropa Şurası daha sonra iki müxtəlif fəaliyyət planını realizə edərək hüquq mühafizə orqanlarının təlim keçməsini və ölkələrdə milli qanunvericiliyin inkişafını təmin etmişdir. Avropa Şurası milli qanunvericilik fəaliyyətləri ilə bağlı əhatəli verilənlər bazası yaratmışdır.

## VII. BMT-NİN FƏALİYYƏTİ

BMT Baş Assambleyası informasiya təhlükəsizliyi ilə bağlı 2000-ci ildən başlayaraq beş müxtəlif qətnamə qəbul etmişdir [12]. Bu qətnamələrdə informasiya texnologiyalarının qeyri qanuni istifadəsinə qarşı mübarizəyə (A/RES/55/63, 2000), üzv ölkələri bu sahədə koordinasiya və əməkdaşlığa, həmçinin onları milli qanunvericiliyi və polis təşkilatlarını təkmilləşdirməyə çağırır. (A/RES/56/121, 2001). Qlobal kibertəhlükəsizlik mədəniyyəti ilə bağlı qətnamədə (A/RES/57/239, 2002) ölkələrdə informasiya cəmiyyəti inkişaf etdikcə kibertəhlükəsizlik tələblərinin də artığı qeyd edilərək kibercinayətkarlıqla mübarizədə hökumətlərlə və hüquq mühafizə orqanları ilə yanaşı bütün tərəfdaşların iştirakının vacibliyi vurğulanır. Növbəti qətnamədə (A/RES/58/199, 2003) qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması və kritik infrastrukturların mühafizəsi məsələsi qabardılmışdır. Burada BMT üzv ölkələri kritik infrastrukturlarla bağlı risklərin azaldılması üçün yeni strategiyalar mənimsəməyə çağırır. Digər bir qətnamədə isə (A/RES/64/211) İnformasiya Cəmiyyəti üzrə Dünya Sammitinin (WSIS) iki mərhələsinin də nəticələri nəzərə alınır [13].

Qeyd etmək lazımdır ki, WSIS tərəfindən sammitin C5 (Building Confidence and Trust in the use of ICTs) istiqaməti üzrə BTİ yeganə moderator təyin olunmuşdur. Nəticədə 17 may 2007-ci il tarixində BTİ Qlobal Təhlükəsizlik Gündəliyi (GCA: ITU Global Cybersecurity Agenda) qəbul dilmişdir [14]. Gündəliyin əsas iş istiqamətləri aşağıdakı kimidir:

1. Qanunvericilik məsələləri (Model qanunlar və s.);
2. Texniki və procedural önləmlər (Proqram təminatları üçün qlobal səviyyədə qəbul edilən akkreditasiya sxemləri, protokollar və standartlar);
3. Kritik informasiya infrastrukturlarına yönəlmiş hücumlara qarşı mübarizə üçün təşkilati və strateji məsələlər;
4. Kibertəhlükəsizlik üzrə milli siyasətin reallaşdırılması üçün tələb olunan bilik və təcrübənin inkişafı məsələləri;
5. Beynəlxalq əməkdaşlıq, dialoq və koordinasiya məsələləri.

BTİ-nin gündəlik çərçivəsində reallaşdırdığı ilk konkret proqram Uşaqların Onlayn Mühafizəsi (COP: The Child Online Protection təşəbbüsüdür [15].

## VIII. NATO ÇƏRÇİVƏSİNDƏ ƏMƏKDAŞLIQ

NATO-nun 2010-cu il Lissabon sammiti kibertəhlükəsizliyi NATO-nun gələcək illərdə qarşılaşacağı ən aktual təhdidlər sırasına daxil etmiş və 2011-ci ildə müdafiə nazirləri kiber-müdafiə üzrə gələcək tədbirlərin konsepsiyasını bəyənmişdir.

2008-ci ildə Tallindəki (Estoniya) kiber müdafiə üzrə qabaqcıl təcrübə mərkəzi NATO tərəfindən "NATO qabaqcıl təcrübə mərkəzi" kimi bəyənilmişdir. Bu mərkəzdə kibertəhlükəsizlik üzrə elmi-tədqiqatlar və təlim tədbirləri həyata keçirilir. Mərkəz kibertəhlükəsizlik sahəsində tədqiqatların aparılmasına xüsusi fikir verir, tədqiqatların əsas istiqamətləri aşağıdakılardır:

- kiberfəzada təhlükəsizliyin təmin edilməsi konsepsiyalarının və strategiyalarının, həm NATO çərçivəsində, həm də ayrıca üzv-ölkələrdə kiber-əməliyyatların (hücum, müdafiə, istismar) aparılması konsepsiyalarının işlənilməsi;
- NATO və üzv-ölkələrin rəqəmsal hesablama sistemlərində təhlükəsizliyin təmin edilməsi, kiber-hücumların aşkarlanması və nəticələrinin aradan qaldırılması sahəsində texniki həllərin işlənməsi, kənardan müdaxilələrin aşkarlanması üsullarının işlənməsi;
- kiber-hücum risqlərinin qiymətləndirilməsi metodologiyalarının işlənməsi, kiber-müdafiə sahəsində təlimlərin və məşqlərin modelləşdirilməsi və keçirilməsi.

## IX. BEYNƏLXALQ KİBERTƏHLÜKƏSİZLİK STRATEGİYALARI

Kibertəhlükəsizlik bir sıra ölkələrdə (məsələn, ABŞ, Avropa Birliyi, Rusiya) xarici siyasətin prioritetlərindən biri elan edilib. ABŞ kibertəhlükəsizliyin azad ticarət və sosial-iqtisadi inkişaf üçün etibarlı, təhlükəsiz və açıq mühit qurmağa imkan verəcək beynəlxalq əsaslarının formalaşdırılması haqqında 2011-ci ildə sənəd hazırlamışdı. Bu sənəddə bir neçə əsas prinsip təsvir edilir [3].

Birinci yerə iqtisadi əlaqələr qoyulub. ABŞ kommersiya sirri daxil olmaqla bu və ya digər tərəfə məxsus olan informasiyanı qorumaqla İnternet üzərindən azad ticarət imkanı yaratmağı təklif edir. Digər vacib prioritet kiberfəzada beynəlxalq davranış kodeksinin yaradılmasıdır. Layihə müəlliflərinə görə, belə kodeksin varlığı xarici haker hücum-larından qorunmağa imkan verəcək. Daha bir bənd kibercinayətkarlıqla mübarizəyə həsr olunub. ABŞ diqqəti konkret cinayətlərə yönəltməyə və İnternetə girişi məhdudlaşdırmamağa çağırır.

Təhlükəsiz mühit formalaşdırmaq imkanı olmayan ölkələrə yardım göstərilməsi də nəzərdə tutulur. Strategiya ABŞ-ın bütün əsas nazirliklərini əhatə edir, onların hamısına xarici ölkələrdə analoji nazirliklərin iştirakı ilə qarşılıqlı əlaqə prinsiplərini yaratmaq tapşırığı verilib.

Hazırda AB üçün vahid kibertəhlükəsizlik strategiyası yoxdur. 2012-ci ildə Avropa Komissiyası AB üçün "İnternetin təhlükəsizliyi strategiyası"nı işləyib hazırlamışdır. Layihədə əsas risqlər və problemlərlə yanaşı, iqtisadi və geosiyasi imkanları aşkarlamaq, üçüncü ölkələrdə İnternetin təhlükəsizliyi probleminə hazırlıq səviyyəsini müqayisə etmək, həlli tələb edilən vacib problemləri müəyyənləşdirmək, cari və planlaşdırılan tədbirləri qiymətləndirmək məqsədləri qoyulur.

Rusiya Federasiyası milli informasiya sistemlərinin mühafizəsi haqqında BMT Konvensiyasının layihəsini hazırlamışdır. Layihədə dünya infromasiya fəzasının normal və stabil inkişafına əsas təhdidlər sadalanır. Layihə müəlliflərinə görə, bu təhdidlər informasiya müharibəsinin elementləri hesab oluna bilər və beynəlxalq sülh və təhlükəsizliyə qarşı cinayət kimi tanınmalıdır.

Konvensiya layihəsində kibertəhdidlərlə beynəlxalq səviyyədə mübarizə aparmağa imkan verən normalar sadalanır. Vurğulanır ki, dövlətlər təhlükəsizliyin bölünməzliyi prinsipinə əməl edəcəklər və öz təhlükəsizliklərini digər dövlətlərin təhlükəsizliyinin ziyanına gücləndirməyəcəklər.

Konvensiyaya görə dövlətlər "informasiya fəzasında təhdidlərin artmasına səbəb ola bilən planların işlənməsi və qəbulundan çəkinməli, digər dövlətin daxili səlahiyyətlərinə qarışmaq üçün İKT-dən istifadə etməməli, digər dövlətlərin daxili işlərinə qarışmaq və müdaxiləni həyata keçirmək üçün böhtanlardan, təhqiredici və ya düşmən təbliğatdan çəkinməlidir."

## X. KOMPÜTER İNSİDENTLƏRİ İLƏ MÜBARİZƏ VƏ TƏHLÜKƏSİZLİK KOMANDALARI (FIRST)

Kompüter insidentləri ilə mübarizə komandaları (CERT) FIRST beynəlxalq federasiyasının çətiri altında birləşərək təhlükəsizlik insidentləri ilə bağlı informasiya mübadiləsi edirlər. FIRST 42 ökədən dövlət, özəl, elm və təhsil qurumlarının 220 CERT komandası bu təşkilatla əməkdaşlıq edir. Təşkilat həmçinin informasiya təhlükəsizliyi sahəsində standartlaşma üzrə əməkdaşlıq edir, həmçinin boşluqlarının analizi vahid qiymətləndirilməsi sistemini istifadə edir [16].

## XI. TƏHLÜKƏSİZ İNTERNET TƏŞƏBBÜSÜ

INSAFE Avropa İttifaqının 27 ölkəsi, İslandiya, Norveç, Rusiya və Serbiyada yerləşən 31 milli məlumatlandırma mərkəzinin şəbəkəsidir. Hər bir məlumatlandırma mərkəzi təhlükəsiz İnternet mühitinin yaradılması üzrə müxtəlif fəaliyyətlərlə uşaqlara və gənclərə xidmət edir. Bu təşkilatın koordinasiyası ilə yardım xətti, qaynar xətt kimi xidmətlər göstərilir və ildə bir dəfə bütün dünyada "Təhlükəsiz internet günü"nü qeyd edir. Avropa birliyi Təhlükəsiz İnternet Proqramına milyonlarla vəsait ayırır və gənclərin daha steril internetə çıxışına imkan verir [17].

## NƏTİCƏ

Araşdırma nəticəsində aydın olmuşdur ki, informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlıq üzrə çox ciddi səylər göstərilmişdir. Birləşmiş Millətlər Təşkilatı, Beynəlxalq Telekommunikasiya İttifaqı, NATO, İnformasiya Cəmiyyəti üzrə Dünya Sammiti, Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi kimi qlobal təşkilatlar və təşəbbüslər ən geniş çərçivədə, FIRST və INSAFE kimi təşkilatlar isə xüsusi istiqamətlər üzrə informasiya təhlükəsizliyinin təmin edilməsi üçün uğurlu addımlar atmışdır.

Dövlətlər də öz növbəsində qanunvericilik fəaliyyətindən konkret əməliyyatlara qədər bütün sahələrdə beynəlxalq çağırışlara dəstək verir və birlikdə informasiya təhlükəsizliyi mühitinin yaranması üçün səy göstərirlər.

İnformasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlıq üçün global müstəvi formalaşsa da, ölkələrin və müxtəlif tipli qurumların daha sıx əməkdaşlıq qurması üçün, xüsusilə də birgə və ani reaksiya tələb edən həssas məsələlərdə daha sıx inteqrasiyaya ehtiyac vardır. Belə əməkdaşlıq mexanizmləri üçün IMPACT kimi təşəbbüslər böyük təcrübə mənbəyi təşkil edir. Həmçinin INSAFE-in təcrübəsində olduğu kimi istifadəçilərin özlərinin təhlükəsizliyin təmin olunması prosesində aktiv rol oynayacağı təşəbbüslərə və layihələrə ehtiyac vardır.

## ƏDƏBİYYAT

[1] http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
[2] ITU National Cybersecurity Strategy Guide, September 2011
[3] N. Choucri, S. Madnick, J. Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," Information Technology for Development, vol. 20, no. 2, pp. 96-121, 2014.
[4] http://www.state.gov/www/issues/economic/summit/communique97.html
[5] http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7
[6] https://www.ic3.gov
[7] http://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html
[8] www.oecd.org/dataoecd/20/4/36871344.ppt
[9] http://www.impact-alliance.org/aboutus/ITU-IMPACT.html
[10] https://www.enisa.europa.eu/about-enisa
[11] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[12] http://www.un.org/documents/resga.htm
[13] http://www.itu.int/wsis/index.html
[14] ITU Global Cybersecurity Agenda (GCA): A Framework for International Cooperation in Cybersecurity, 2007
[15] http://www.itu.int/cop/
[16] https://www.first.org
[17] http://www.saferinternet.org/