TURKPA

PARLIAMENTARY ASSEMBLY OF TURKIC-SPEAKING COUNTRIES

HÜQUQ MƏSƏLƏLƏRİ VƏ BEYNƏLXALQ ƏLAQƏLƏR KOMİSSİYASI

BEŞİNCİ İCLAS

ANKARA-2016

HESABAT MƏRUZƏSİ

“Kiber Cinəyatkarlığa Qarşı Mübarizə: Üzv Ölkələr Arasında Hüquqi Çərçivənin və Əməkdaşlığın İnkişaf Etdirilməsi“

GİRİŞ

Məlumat texnologiyalarının təsir etdiyi qloballaşma və buna bağlı olaraq meydana gələn yeni problemlər, hər dövlət və hər fərd üçün əsas məsələ halını almaqdadır. Bu səbəblə kompüter şəbəkələrinin davam edən yaxınlaşması, qloballaşması və artan rəqəmsal mühit yeni dəyişiklikləri nəzərə almağı tələb edir. Texnologiyanın inkişafı yeni fürsətlərin qapısını açır və bununla yanaşı bu kimi halların genişləndirilməsi informasiya sahəsinə cinayət anlayışını gətirir. Məlumat texnologiyalarından asılılıq həyatın demək olar ki, hər sahəsində hər il artmaqdadır və kiber sahə və cinayətlərlə əlaqədar problemlər daha da qlobal bir xüsusiyyət kəsb etməkdədir.

Nəticə olaraq, kiber təhlükəsizlik riskləri bu əsrdə bir sıra iqtisadi və milli təhlükəsizlik problemlərini ortaya çıxarmaqdadır. Bu sürətli dəyişmə ilə birlikdə Kiber Cinayət anlayışı ölkələrin gündəliyində əhəmiyyətli bir yer tutmaqdadır.

Hüquq Məsələləri və Beynəlxalq Əlaqələr Komissiyasının texnoloji irəliləyişlərin təsirləri və nəticələri ilə əlaqədar 29 aprel 2015-ci il tarixində Bişkekdə keçirilən Dördüncü Toplantısında TürkPA üzvü ölkələrində kiber cinayətlərlə mübarizə və hüquqi çərçivə probleminin, bu prosesdə qanunvericilik ölçüsü ilə parlamentin töhfəsi perspektivilərinin ələ alınmasına qərar verilmişdir.

Beləliklə Komissiyanın 2016-ci ilin may ayında Ankaradakı Beşinci Toplantısı, Assambleyanın 2016-cı il sentyabr ayında Bişkekdə keçiriləcək Yeddinci Plenar İclasında təqdim olunacaq hesabat məruzəsi və tövsiyə qərarının müzakirəsi məqsədi ilə "Kiber Cinəyatkarlığa Qarşı Mübarizə: Üzv Ölkələr Arasında Hüquqi Çərçivənin və Əməkdaşlığın İnkişaf Etdirilməsi" mövzusuna həsr olunmuşdur.

KİBER CİNAYƏTLƏRLƏ MÜBARİZƏ VƏ TÜRKPA ÜZVÜ ÖLKƏLƏRİNDƏ QANUNVERİCİLİK

1. Yeni məlumat texnologiyaları ilə kosmos və zaman sıxışdırılır, bununla birlikdə bol miqdarda qlobal məlumata işıq sürətində giriş və bir anlıq məlumat mübadiləsi imkanı təmin edilir. Bu səbəbdən müasir dünyada kiber sahə praktikada hər şeyə və hər kəsə toxunur. Ancaq qarşılıqlı bağlantılardakı bu genişlik, bir yerdəki problemin başqa bir yerdəki kompüterlərə təsir potensialının da olduğu və texnoloji inkişafla birlikdə kiber təhlükəsizlik və kiber cinayət üzrə narahatlıq mənasını verməkdədir.

2. Elektron məlumat axışı və şəbəkələri demək olar ki, həyatın hər sahəsində kök salmışdır. Qlobal səviyyədə bir-birinə bağlanmış olan ünsiyyət infrastrukturu, günümüzün fəaliyyətlərinin az qala hamısında yer tapır və iqtisadiyyat, vətəndaş infrastruktur, ictimai təhlükəsizlik və milli təhlükəsizlik üçün kritik dəstək təmin edir.

3. Diğer yandan, bilgisayar ve iletişim alanındaki gelişmeler, karmaşık siber güvenlik sorunlarından bazılarını öne çıkarır olmuştur. Daha gevşek düzenlenmiş dijital

altyapının daha çok kişiye ulaşmasıyla birlikte birtakım açıklar daha fazla risk oluşturmaktadır. Siber saldırılar, maruz kalınan açıkları yıkıcı niteliklere dönüştürebilmekte ve ciddi sonuçlara yol açabilmektedir.

4. İqtisadi və milli təhlükəsizlik informasiya texnologiyası və məlumat infrastrukturundan daha çox asılı hala gəlməkdədir. Şəbəkələrdən ibarət bir quruluş, iqtisadiyyatın bütün sektorlarının, başqa bir deyişlə enerji (elektrik gücü, neft və qaz), nəqliyyat (dəmir yolu, hava yolu, dənizyolu), maliyyə və bank, informasiya və telekommunikasiya, əhalinin sağlamlığı, fövqəladə xidmətləri, su, kimya, müdafiə, sənaye, qida, kənd təsərrüfatı və poçt xidmətlərinin işləyişinə dəstək olacaq. Eyni zamanda bu strukturlar elektrik transformatorlarınına, boru kəmərlərinə, radarlara və.s nəzarət edir.

5. Başda dövlət orqanları olmaqla bütün təşkilat və qurumların bir çox xidmətlərini internet mühitində təqdim etməyə başlamasıyla birlikdə bu mühitdə yaşanacaq mənfiliklər fərdi, ictimai və iqtisadi həyata əhəmiyyətli dərəcədə təsir etməyə başladı. Meydana gələ biləcək hadisələr həm maddi, həm də mənəvi zərərlərə səbəb ola bilər. Bu səbəbdən məlumat şəbəkələrinə edilən kiber hücumlar, kritik fəaliyyətlər üzərində ciddi nəticələrə yol açа bilər. İndiki vaxtda getdikcə artan bu risklər kiber cinayətlərə qapı açır.

6. Kiber cinayətlərlə mübarizə sahəsində müxtəlif beynəlxalq təşkilatlar və təşkilatlar nəzdində dünya səviyyəsində bir çox QHT-lərin təşəbbüsü, eyni zamanda həyata keçirilən bir çox işin olması, problemin həm ciddiliyini, həm də bu mövzuya istənilən həllin tapılmamasında nə qədər çox səy sərf etmək lazım olduğunu göstərir. Bu günə qədər təmin edilən inkişaf nəzərə çarpan dərəcədə olmaqla birlikdə, kiber cinayətlə təsirli bir mübarizədə hələ çox məsafə qət edilməsi lazım olduğu deyilməlidir.

7. Ümumi olaraq görülən işlərdə kiber cinayət anlayışının informasiya texnologiyalarının inkişafı ilə ortaya çıxan və ya informasiya texnologiyalarının istifadə edilməsi ilə işlənən cinayətləri ifadə edən çətir bir anlayış olaraq istifadə edildiyi görülməkdədir. Bunlar; birbaşa informasiya texnologiyalarını və məhsullarını hədəf alan, *(icazəsiz giriş, məlumatlara və ya məlumat sistemlərinə zərər verilməsi vs.)* və ya informasiya / informasiya texnologiyası istifadə edilərək işlənən cinayətlər *(fırıldaqçılıq, şəxsiyyət kredit kartı və s)* və məzmunla əlaqədar cinayətlər *(Uşaq pornoqrafiyası və ya irqçi məzmunların yayımlanması və ya saxlanılması cinayətləri kimi)* olaraq geniş bir sahədə qiymətləndirilməkdədir.

8. Uzun bir siyahıya sahib kiber cinayətlərlə mübarizə sahəsini ələ alarkən yenilikçi bir yanaşmanı inkişaf etdirmək vacibdir. Kiber cinayətkarlığa və kiber terrorizmə qarşı rəqəmsal cəbhə ilə yanaşı fərdi, ictimai və siyasi cəbhələrdə də mübarizə aparılmalıdır.

9. Kiber təhlükəsizlik və cinayətlərlə mübarizə siyasəti, təhdidləri yüngülləşdirmə, beynəlxalq iştirakın, sürətli reaksiyanın və kompüter şəbəkəsi əməliyyatları, informasiya təhlükəsizliyi, hüquqi sanksiyaları kimi geniş bir sahəni əhatə etməlidir, çünki bu mövzular qlobal informasiya və rabitə infrastrukturunun təhlükəsizliyi və stabilliyi ilə əlaqəlidir.

10. Kiber sahədəki çatışmazlıqları ələ almaq və informasiya texnologiyaları inqilabının tam potensialının qlobal birlik tərəfindən görülməsini təmin etmək hökumətlərin əsas məsuliyyətidir. Hökumətlər bir tərəfdən iqtisadi tələblər və milli təhlükəsizlik tələblərini təmin edərkən, digər tərəfdən də kiber təhlükəsizlik sahəsindəki və buna istiqamətli olaraq çıxan cinayət və qanun pozuntularına qarşı mübarizədə köməkçi olacaq araşdırmalara daha çox investisiya etməlidirlər. Təhdidlər və risklər haqqında daha çox ictimai şüur yaratmaq və kiber sahədə təhlükəsizliyə istiqamətli bütöv bir yanaşma inkişaf etdirmək də əhəmiyyətlidir.

11. TÜRKPA üzv dövlətləri, kiber təhlükəsizlik və cinayətkarlığa qarşı mübarizəsində digər bir çox ölkədə olduğu kimi tədbirlər görür. Bir tərəfdən təhlükəsizliyi, hüquq-mühafizə və məxfilik hüquqlarını dəstəkləyərkən digər tərəfdən də innovasiya və texnoloji tərəqqini təşviq edən bir mühiti qoruma paradoksu ilə üz-üzədir

12. Avropa Şurası "Virtual Mühitdə İşlənən Cinayətlər Müqaviləsi"- ni imzalayaraq ratifikasiya edən Türkiyədə məsələ ilə əlaqədar Nəqliyyat, Dənizçilik və Kommunikasiya Nazirliyi tərəfindən "Milli Kiber Təhlükəsizlik İşlərinin Aparılması, İdarə Edilməsi və Koordinasiyasına Dair Qərar" layihəsi hazırlanmışdır. İnformasiya Texnologiyaları və Rabitə İdarəsi ilə Nəqliyyat, Dənizçilik və Kommunikasiya Nazirliyi və Türkiyə Elmi və Texniki Araşdırma Qurumunun əməkdaşlığında digər Nazirliklərin də iştirakı ilə hər il Milli Kiber Təhlükəsizlik Təlimləri keçirilir. 2012-ci ilin İyul ayında Türkiyə Elmi və Texniki Araşdırma Qurumu - İnformasiya Təhlükəsizliyi İrəli Texnologiyalar Araşdırma Mərkəzinin nəznində "Kiber Təhlükəsizlik İnstitutu" yaradılmışdır.

13. Türkiyədə informasiya və internet mühitində işlənən cinayətlər ilə əlaqədar mövcud qanunvericilik qiymətləndirildiyində, 5237 saylı "Türk Cəza Qanunu", 5651 saylı "İnternet mühitində edilən Yayınların təşkil edilməsi və Bu Nəşrlər Yoluyla İşlənən Cinayətlərlə Mübarizə Edilməsi Haqqında Qanun", 5070 saylı "Elektronik İmza Qanunu" kimi qanunlar və müvafiq əsasnamələrlə kiber təhlükəsizlik hüquqi bazasının dəstəkləndiyi görülür.

14. Azərbaycan Respublikası Avropa Şurası "Virtual Mühitdə İşlənən Cinayətlər Müqaviləsi"-ni (Budapeşt Konvensiyanı) 30 Sentyabr 2009-ci tarixində ratifikasiya etmiş və bu konvensiya Prezidentin imzası ilə qüvvəyə minmişdir. Bununla yanaşı Azərbaycan 1981-ci ildə Avropa Şurası tərəfindən Strasburq şəhərində “Fərdi məlumatların avtomatlaşdırılmış qaydada işləməsi ilə əlaqədar şəxslərin qorunması haqqında” Konvensiyaya daxil olmuş və bu öz əksini 209 saylı qanunda tapmışdır. Həmçinin "Elektron İmza" və "Dövlət Sirri" haqqında qanunlar bu sahədə atılmış mühüm hüquqi addımlardır.

15. Azərbaycan Cinayət Məcəlləsində birbaşa kiber cinayətkarlıq mövzusuna toxunan maddələr mövcuddur. (30.Hissə, 271,272,273-cü Maddələr). Burada icazəsiz giriş, zərərli məlumatların və proqramların yayılması kimi mövzular üzərinə hökmlər yer alıb. Yenə eyni qanunda təhqir və ləyaqəti

yaralayıcı nəşrlərlə əlaqədar, internet məkanını da tam əhatə edici şəkildə təşkil edilərək cəza hökmləri yer almışdır. Həmçinin Azərbaycan İnzibati Cinayətlər haqqında qanunun (147 və 148-ci Maddələr) 16-ci Hissəsi "İnformasiyadan istifadə edilməsi, yayımı və qorunmasına zərər verən qəbahətlər çərçivəsində, məlumatların istifadəsi, sui-istifadəsi, bölüşdürülməsi və qorunması" haqqında müddəalar ehtiva edir. Bununla yanaşı informasiya texnologiyalarının istifadəsində yaşanan pozuntulara işarə edən digər maddələr də qanunda yer almaqdadır.

16. Qazaxıstan Prezidenti tərəfindən imzalanaraq 1 Yanvar 2015-ci il tarixi etibarı ilə qüvvəyə minən Qazaxıstan Respublikasının yeni Cinayət Məcəlləsində kiber cinayətlər üçün cinayət məsuliyyətinə cəlb edilməsi dair xüsusi bölmə mövcuddur. Bura icazəsiz kompüter məlumatlarına giriş, qanunsuz faktların əldə edilməsi, silinməsi və dəyişdirilməsi, cəmiyyətə zərər vermək potensialına malik proqram və göstəricilərin yayılması məsələləri daxildir. Həmçinin Cinayət Məcəlləsində böhtan xarakterli və təhqiredici məlumatları əhatə edən maddələr mövcuddur. Bununla yanaşı, kiber cinayətlərlə mübarizə üzrə əməkdaşlıq Müstəqil Dövlətlər Birliyi (MDB) çərçivəsində aparılır və bu sahədə beynəlxalq səviyyədə başqa sənədlər də imzalanmışdır.

17. Qırğızıstan Respublikasının Cinayət Məcəlləsində "İnformasiya texnologiyaları sahəsində törədilən cinayətlər" məqamını bilavasitə ehtiva edən üç maddə yer alır(28-ci Hissə).Qırğız Respublikası İnzibati Məsuliyyət Qanunu çərçivəsində 21-ci hissəsi "Telekommunikasiya şəbəkələri və ünsiyyətin əməliyyat və istifadə qaydalarını mövzu seçən pozuntular" adı altında təşkil edilmişdir.

18. Dövrümüzün kiber problemlərlə mübarizədə təkcə milli qanunların qəbul edilməsi və tətbiqi yetərsiz qalır. Kiber cinayətlərlə mübarizə haqqında daimi qanunların və əsasnamələrin qəbul edilməsi və bunların lazım olduğu yerlərdə və zamanlarda normal hala gətirilməsi lazımdır. Buna səbəb kimi informasiya və kommunikasiya şəbəkələri, həm milli, həm də beynəlxalq səviyyədə böyük ölçüdə özəl sektorun mülkiyyətindədir və yenə də özəl sektor tərəfindən istifadədə olduğu göstərilə bilər. Bu səbəbdən kiber təhlükəsizlik problemlərinin müzakirə olunmasında, kiber sahəni zəmanət altına almağa kömək edəcək dövlət - özəl sektor tərəfdaşlığı ilə birlikdə beynəlxalq əməkdaşlıq və normalar, inkişaf etdiriləcək strategiyaların əsas faktoru olacaqdır.

19. Parlamentlər, kiber sahə və kiber cinayətlərlə mübarizə məsələsində qayğılarını səslərini eşitdirmələri və davamlı inkişafın mühüm vasitəsi olaraq kiber təhlükəsizliyi təmin etməyə yönəlik tədbirlərin artırılmasına daha çox kömək etmələri lazımdır.

20. Bir tərəfdən ola biləcək kiber hücumlardan irəli gələn zərərləri minimuma endirərkən və yüngülləşdirərkən digər tərəfdən də texnoloji tərəqqinin faydalarının geniş bir şəkildə başa düşülməsini və dəstəklənməsini təmin etmək məqsədilə kiber təhlükəsizlik və kiber cinayətlər sahəsində əhatəli bir

milli maarifləndirmə yaradacaq şəkildə mövcud hüquqi mexanizmləri ən yüksək səviyyədə istifadə etmələri lazımdır.

21. Kiber hücumlara və müdaxilələrə qarşı mübarizədə müvafiq qurumlara kifayət qədər dəstək ola bilmək üçün hüquq-mühafizə və təhlükəsizlik qurumları və məhkəmə sistemi arasında qarşılıqlı təsirin və koordinasiyanın inkişaf etdirilməsinə də xüsusi əhəmiyyət verilməlidir.

22. Üzv ölkə parlamentlərin, kibernetik təhdidlərə və kiber cinayətkarlığa qarşı kompakt bir qarşı hərəkətə keçilməsi üçün beynəlxalq strategiya inkişaf etdirilməsinə rəhbərlik etmələri və bu etibarla milli cəza qanunlarının uyğunlaşdırılması üçün birgə beynəlxalq hüquqi mexanizmlərin təkmilləşdirilməsinə ehtiyac var.

23. Kiber təhlükəsizlik sahəsindəki qanunların beynəlxalq standartlarla qanuna uyğun hala gətirilməyə davam edilməsi mühüm əhəmiyyət kəsb edir. Bununla bərabər elmi və texnoloji tərəqqi əsasında davamlı inkişaf etdirməklə bağlı beynəlxalq əqdlərin qəbul olunmasında da fəal rol oynamaları və bu hökmləri milli qanunvericiliyə köçürmələri də əhəmiyyətlidir.

Beynəlxalq Fəaliyyət

Kiber təhlükəsizlik, informasiya təhlükəsizliyi və şəbəkə təhlükəsizliyi mövzusunda yaşanan qlobal problemlər və ortaya çıxan kiber cinayətlər əlaqədar olaraq ancaq əsas maraqlı tərəfləri əhatə edən beynəlxalq əməkdaşlıq strategiyası və kiber təhlükəsizlik mədəniyyəti ilə müzakirə edilə bilər. Bir çox ölkəyə eyni anda təsir göstərən kiber cinayətlərlə mübarizə aparmaq məqsədilə beynəlxalq dialoq və əməkdaşlığa olan ehtiyac danılmazdır.

24. Beynəlxalq kiber cinayətlərlə mübarizə ilə əlaqədar alətlərdən biri Avropa Şurası (AŞ) nəzdində hazırlanaraq 23 noyabr 2001-ci il tarixində Budapeştdə imzalanmaq üçün açılan və 1 iyul 2004-cü ildə qüvvəyə minən "virtual mühitdə işlənən cinayətlər Müqaviləsi" dir. Bu Müqavilə / Konvensiya, kiber cinayətlərlə mübarizədə milli hüquqi çərçivələrin uyğunlaşdırılması və beynəlxalq əməkdaşlığın ünsürləri barəsindədir. Bu hüquqi akt həm uyğunlaşdırma, həm də siyasi cəhətdən əhəmiyyətlidir. Konvensiyada kiber cinayətlərə qarşı milli hüquqi çərçivənin inkişaf etdirilməsinin əsas xüsusiyyətləri nəzərdə tutulduğuna görə Avropa normaları baxımından əhəmiyyətli bir vasitədir. Bununla yanaşı Konvensiyanın imzalanması, kiber cinayətkarların xaric edilməsi də daxil olmaqla, əməliyyat məsələləri sahəsində beynəlxalq əməkdaşlığı asanlaşdırır. Avropa Şurası, bütün dünyada Müqavilə /Konvensiyanı dəstəkləmək üçün xüsusi sektorla və üzv dövlətlərlə birlikdə bir Qlobal Layihə başlatmışdır. Konvensiyada daha çox sayda ölkənin iştirak etməsi, kiber hücumlara sponsorluq edən cinayətkar qruplar və orqanlar üçün ciddi bir daşındırıcılıq ünsürü meydana gətirir.

25. Avropa İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (OECD) Məlumat Təhlükəsizliyi və Məxfiliklə bağlı Hökumətlərarası İş Qrupu (WPISP), məlumat cəmiyyəti və müqavimətin inkişaf siyasəti barəsində tövsiyə qərarları və hesabatlar hazırlayır. Hökumət, iş dünyası və sivil toplumların mütəxəssislərdən ibarət şəbəkə üzərindən meylləri yoxlayır və məlumat mübadiləsini asanlaşdırır. Avropa İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı OECD, texnologiyanın məlumat təhlükəsizliyi və gizlilik üzərindəki təsirlərini analiz edən nizamlı hesabatlar dərc edir.

26. ATƏT kiber təhlükəsizliklə bağlı danışıqlara 2008-ci ildə başlamışdır. O zamandan bəri ATƏT-in iştirakçı dövlətləri, əsas məsələlər kimi ölkələrin kiber cinayətlər və terrorizmlə mübarizə qabiliyyətlərinin inkişaf etdirilməsi ehtiyacının və kiber sahədə məsul dövlət rəftarının təyin edilməsinin müzakirə edildiyi bir neçə iclas keçirmişdir. ATƏT-in ölkələrinin, kiber təhlükəsizlik mövzusuna yanaşmalarında çox fərqli maraq sahələri və dünyagörüşləri var və ATƏT-in bu mübahisədəki tam rolunun nə olacağı barəsində tam bir razılıq meydana gəlməmişdir.

27. BMT Təhlükəsizlik Şurası, kiber təhlükəsizliyə uyğun qərarlar qəbul etmişdir. BMT Sosial və İqtisadi Komissiyası çərçivəsində 56/121 saylı "İnformasiya Texnologiyalarından sui-istifadə cinayəti ilə Mübarizə" və 57/239 saylı "Qlobal Kiber Təhlükəsizlik Mədəniyyətinin Yaradılması" qərarlarını qəbul edilmişdir. Hər iki qərar da beynəlxalq əməkdaşlığın əhəmiyyətini, kiber cinayətkarlar üçün etibarlı dayaqların aradan qaldırılması, təhlükəsizliyin tətbiq edilməsində əməkdaşlıq və kiber təhlükəsizlik mövzularında ümumi məlumatlılığın artırılması ehtiyacını vurğulayır. "Qloballaşma və qarşılıqlı asılılıq: inkişaf üçün elm və texnologiya" haqqında 64/422 saylı Qərar, eyni zamanda BMT ölkələrinin öz kiber təhlükəsizliklərini qorumağa istiqamətli qiymətləndirmə araşdırmasından ibarətdir. Bu cəhdlər, kiber təhdidlər mövzusunda artan qayğılara diqqət çəkmiş, qlobal bir maarifləndirmə meydana gətirməyə köməkçi olmuş və BMT ölkələrini kiber təhlükəsizlik mövzusunda öz milli mexanizmlərini irəliyə daşımaları üçün lazımlı tədbirlər görməyə yönəlmişdir.

III. NƏTİCƏLƏR

- ✓ Bu gün şəxs, təşkilat və qurumlara aid məlumat aktivlərinin həcmi və çeşidinin keçmişə nəzərən ciddi artımlar göstərdiyi aydındır. Artıq məlumatlar çox böyük ölçüdə rəqəmsallaşdığından, bu vəziyyət həm ictimai, həm də özəl iş müddətlərini asanlaşdırmaqdadır. Lakin, bununla yanaşı, keçmişdə mümkün olmayan yeni xidmətlərin mümkün hala gətirilməsində, kiber təhlükəsizlik və kiber cinayətlərlə mübarizə mövzusunun ciddi bir problem olduğu qəbul olunur və lazımi tədbirlərin təxirə salınmadan keçirilməsinə ehtiyac duyulur.

- ✓ Kiber sahədə milli sərhədlər çox az məna kəsb edir. Kiber sahənin qlobal xüsusiyyətindən doğan mövcud zəifliklər dünyanın gözü qarşısında cərəyan edir və sui-istifadə etmək üçün kifayət qədər qabiliyyəti olan hər kəs tərəfindən əlçatandır. Kiber mühitdə təcavüzkar və zərər çəkənin əksər hallarda fərqli ölkələrdə yerləşməsi, dolayısı

ilə kiber cinayətlərlə mübarizə və təhlükəsizlik, beynəlxalq qarşılıqlı fəaliyyət mexanizmlərinin və sazişlərinin əhəmiyyət kəsb etdiyi cinayət məqsədli sui-istifadə sahəsində dövlətlər arasında daha sıx əlaqə və əməkdaşlıq ehtiyacının qarşıya qoyulması və bununla əlaqədar beynəlxalq və regional təşkilatların oynaya biləcəyi rolun vurğulanması mühümdür.

- ✓ Ölkələr bir tərəfdən təhlükəsizlik və gizlilik haqlarını dəstəkləyərkən, digər tərəfdən də innovativ və texnoloji inkişafı təşviq edən bir mühiti qorumaq paradoksu ilə üz-üzədir. Kiber təhlükəsizliyin təmin edilməsi həm milli, həm də beynəlxalq səviyyədə dövlətlər, müəssisələr və cəmiyyət üçün əsaslı bir problemdir.

- ✓ Kiber şəbəkələr istiqamətlənmiş hücumların daha çox sayda olması təhlükəsiz və davamlı bir kiber mühitin yaradılması və kiber təhlükəsizlik bilgisi və yeniliklərin dəstəklənməsi üçün qanunvericiliyin təkmilləşdirilməsi qənaətini meydana gətirir. Beynəlxalq hüquq normalarının milli səviyyədə ratifikasiya olunaraq dəyişdirilməsi kibercinayətkarlığa qarşı mübarizəni sistemləşdirmək istiqamətində zəruri addımdır.

- ✓ Lazımi qanunvericilik hazırlanarkən ictimai və özəl sektorun iştirakı əsas faktordur. İctimai – özəl sektorun iştirakı maarifləndirmə, təhsil, texnoloji inkişaf, zəifliklərin aradan qaldırılması və yenilənmə fəaliyyətləri həyata keçirilən zaman müxtəlif formalarda ola bilər.

- ✓ Kiber təhlükəsizlik və cinayətlərlə mübarizənin qanunvericiliyinin hazırlanmasında hüquq, texniki, sosial-psixoloji ekspertlər və başqa fərqli sahələrdən olan mütəxəssislərin töhfə verməsinin hüquqi və texniki infrastrukturunun təmin edilməsi çox vacib məsələdir.

- ✓ Ölkələrimizdə kiber təhlükəsizlik hüququ mövzusunda daha çox mütəxəssisin yetişdirilməsinə ehtiyac var. Bu baxımdan mövzu ilə əlaqədar sertifikat və diplom işləri ilə təmin edən universitet və institutlar daha çox səmərə gətirəcək və prosesin sağlam idarə edilməsinə böyük töhfə verəcəkdir. İctimai və özəl sektor ayrı-seçkiliyi etmədən Kritik İnfrastrukturun qorunması üçün hüquqi və texniki qaydaların ayrıca və təxirə salmadan yerinə yetirilməsi çox əhəmiyyətlidir və bu mövzuda həyata keçiriləcək elmi işlərin dəstəklənməsi böyük fayda verəcəkdir.

- ✓ Qlobal səviyyədə kiber cinayətlərlə mübarizədə kiber təhlükəsizlik mədəniyyətinin təşviq edilməsi, dəstəklənməsi, inkişaf etdirilməsi və həyata keçirilməsi gərəkdir.

- ✓ TÜRKPA üzv dövlətləri kiber cinayətlə mübarizə üçün ~~ortaq~~ hüquqi çərçivənin təkmilləşdirilməsi üzərində işləməli, bunula yanaşı, məlumat şəbəkəsinin qorunması məqsədilə müştərək fəaliyyətin inkişaf etdirilməsi üçün sıx əməkdaşlıq etməlidir.