Pedaqoji Universitetin Xəbərləri. Humanitar, ictimai və pedaqoji-psixoloji elmlər seriyası –2022, C.70, №4, s. 77-87
Transactions of Pedagogical University. Series of humanitarian, social, pedagogical and psychological sciences – 2022, V.70, №4, pp. 77-87

UOT 004

Z.N.Zəkəryəyev
Heydər Əliyev adına Hərbi İnstitut
aahmkonfrans@gmail.com

KİBER TƏHLÜKƏSİZLİK VƏ KİBERHÜCUMLARA QARŞI MÜBARİZƏDƏ DÖVLƏTLƏRİN DAVRANIŞLARI

Açar sözlər: *kiber təhlükəsizlik, kiber hücum, kiber təhdid, kibermәkan, milli təhlükəsizlik*

Son dövrlər texnologiyalarının sürətlə inkişafı həm də kibertəhlükəsizlik problemini daha çox genişləndirir. Məsələnin getdikcə mürəkkəbliyi onunla mübarizəni də çətinləşdirir. Bu istiqamətdə effektiv addımların atılması üçün ilk öncə onun konseptual olaraq öyrənilməsini zəruri edir. Məqalədə əsas diqqət kibertəhlükəsizliklə bağlı anlayışlara yönəldilmiş, bu anlayışların mahiyyəti izah olunmuş və ona yanaşmalar göstərilmişdir. İşdə bir çox mütəxəssislərin informasiya təhlükəsizliyi və kibertəhlükəsizlik siyasəti ilə bağlı fikirlərinə istinad olunmuş və təhlillər aparılmışdır. Beynəlxalq təhlükəsizliyin təmini üçün dövlətlərin kiberhücumlara qarşı mübarizədə davranışlarının mühüm tərəfləri qeyd olunmuşdur. Xüsusilə də, beynəlxalq əməkdaşlığın, birgə fəaliyyətin, beynəlxalq hüquqa riayət olunmanın vacibliyi məsələsinə diqqət göstərilmişdir.

З.Н.Закаряев

КИБЕРБЕЗОПАСНОСТЬ И ПОВЕДЕНИЕ ГОСУДАРСТВ В БОРЬБЕ С КИБЕРАТАКАМИ

Ключевые слова: *кибербезопасность, кибератака, киберугроза, киберпространство, национальная безопасность*

Стремительное развитие новейших технологий также расширяет проблему кибербезопасности. Возрастающая сложность проблемы затрудняет ее решение. Для того чтобы предпринять эффективные шаги в этом направлении, необходимо сначала изучить его концептуально. В статье основное внимание уделяется понятиям, связанным с кибербезопасностью, разъясняется сущность этих понятий и показаны подходы к ней. В работе были приведены и проанализированы мнения многих экспертов относительно информационной безопасности и политики кибербезопасности. Отмечены важные аспекты поведения государств в борьбе с кибератаками для обеспечения международной безопасности. В частности, внимание было уделено важности международного сотрудничества, совместных действий и соблюдения норм международного права.

Z.N.Zakaryayev

CYBER SECURITY AND BEHAVIOR OF STATES IN COMBATING CYBER ATTACKS

Keywords: *cyber security, cyber attack, cyber threat, cyberspace, national security*

The rapid development of recent technologies also expands the problem of cyber security. The increasing complexity of the issue makes it difficult to deal with it. In order to take effective steps in this direction, it is first necessary to study it conceptually. In the article, the main focus is on concepts related to cyber security, the essence of these concepts is explained and approaches to it are shown. In the work, the opinions of many experts regarding information security and cyber security policy were referred to and analyzed. Important aspects of states' behavior in the fight against cyber-attacks for ensuring international security have been mentioned. In particular, attention was paid to the importance of international cooperation, joint action, and compliance with international law.

Giriş

Son illərdə cəmiyyətin demək olar ki, bütün sahələrinə nüfuz edən informasiya-kommunikasiya texnologiyaları bir sıra hadisələrin və proseslərin səbəbkarına çevrilib. İT texnologiyalarının inkişaf səviyyəsi daha çox dövlətin beynəlxalq aləmdəki rolunu müəyyən edir. Cəmiyyətin qlobal informasiyalaşdırılması XXI əsrdə bəşər sivilizasiyasının inkişafında üstünlük təşkil edən tendensiyalardan biridir.

Bununla belə bu fenomenin bir mənfi tərəfi də var. Göründüyü kimi, informasiya texnologiyalarının həyatın bütün sahələrinə cəlb edilməsi cəmiyyəti ən müasir texnologiyalardan asılı vəziyyətə salır. Kritik infrastrukturun təhlükəsizliyi hazırda onun informasiya və telekommunikasiya komponentinin işləməsinin etibarlılığından birbaşa asılıdır. Bundan əlavə aydındır ki, müasir informasiya texnologiyaları bir sıra xüsusiyyətlərinə və üstünlüklərinə görə cinayət, terror və hərbi məqsədlər üçün istifadə oluna bilməsi hazırkı milli və beynəlxalq təhlükəsizliyə yeni çağırışlar sırasında qlobal və milli səviyyədə kibertəhlükəsizliyin təmin edilməsi problemini ön plana çıxarır.

İşin kifayət qədər aktual olmasını bu cür təqdim etmək olar: birincisi, informasiya texnologiyaları sahəsində köklü dəyişikliklər və prioritetlərin kiberməkana doğru dəyişməsi, sosial, iqtisadi və siyasi məqsədlərə çatmaq üçün kompüter texnologiyaları və internetdən fəal şəkildə istifadə olunması. İkincisi, iştirakçıların dünyanın istənilən yerindən müxtəlif ölkələrin informasiya sistemlərini təhdid etmək imkanına malik olduğu kiberməkanın transmilli xarakteri, nəticədə onlarla mübarizə aparmaq üçün yüksək səmərəli beynəlxalq əməkdaşlığa ehtiyacın olması. Üçüncüsü, kibercinayətkarlıq, kiberterrorizm və

kiberekstremizmin miqyasının genişlənməsi, həmçinin kiberməkandan hərbi məqsədlər üçün istifadə təhlükəsinin genişlənməsi.

Məqalədə əsas məqsəd texnoloji inkişafin kiber təhlükəsizliyə təsirini öyrənmək, kiberhücumların qarşısının alınmasında dövlətlərin məsuliyyətli davranışlarını müəyyən etməkdən ibarətdir. Tədqiqatın obyekti kibertəhlükəsizlik və onun təmin olunması sistemidir. Predmeti texnoloji inkişafın kibertəhlükəsizliyə təsirləri, kibertəhlükəsizliyin pozulması və dövlətlərin kiberməkanda məsuliyyətli davranışlarının müəyyən edilməsidir. Bu məqsədə nail olmaq üçün işdə aşağıdakı vəzifələrin həlli qarşıya qoyulmuşdur: Kibertəhlükəsizlik anlayışlarına yanaşmaları müəyyən etmək; Rəqəmsal infrastrukturun diversifikasiyasının kibertəhlükəsizliyin vəziyyətinə təsirinin qiymətləndirilməsi; Beynəlxalq kibertəhlükəsizlik kontekstində kiberhücumlara qarşı mübarizədə dövlətlərin kiberməkanda məsuliyyətli davranışının tənzimlənməsi mexanizmlərini müəyyən etmək. Mövzunun genişliyi və daha dərindən araşdırma tələb etməsini nəzərə alaraq, məqalənin həcminə uyğun olaraq qoyulan problemin müəyyən məqamlarına yer ayrılmışdır. Gələcəkdə hər bir dövlətin timsalında problemi həm nəzəri, həm də praktik baxımdan ərtaflı tədqiqini həyata keçirmək məqdədəmüvafiq olardı.

Tədqiqatın metodoloji əsasını müasir politologiyada istifadə olunan ümummətiqi və nəzəri metodlar təşkil edir. Kiberməkanda təhlükəsizlik sahəsində tənzimləyici və hüquqi aspektləri müəyyən etmək və təhlil etmək üçün institusional yanaşmadan istifadə edilmişdir. Sistemli yanaşma müasir dövlətlərin kibertəhlükəsizlik siyasətini bir-biri ilə əlaqəli elementlərdən ibarət vahid şəkildə təqdim etməyə imkan vermişdir. Xüsusilə beynəlxalq təhlükəsizlik kontekstində kibertəhlükəsizliyin təmin edilməsində dövlətlərin mövqelərindəki fərqləri və yaxınlaşma məqamlarını müəyyən etmək üçün müqayisəli yanaşmadan istifadə edilmişdir. Tarixi təhlil müasir dövlətlərin kibertəhlükəsizliyin təmin edilməsinə yanaşmalarının təkamülünü, kibertəhlükələrin və kibertəhdidlərin xarakterini təsvir etməyə imkan yaratmışdır. Təsviri metoddan kibertəhlükələrin və kibertəhdidlərin məzmununu aşkar etmək üçün istifadə olunmuşdur.

Məqalədə kibertəhlükəsizlik strategiyasının beynəlxalq cəmiyyətin məqsədlərinə zidd olmadığı, qlobal səviyyədə kibertəhlükəsizlik problemləri ilə mübarizəni dəstəklədiyi analiz edilmişdir.

1. "Kibertəhlükəsizlik" anlayışları və onlara yanaşmalar. İnformasiya-kommunikasiya texnologiyalarının sürətli inkişafı dünyanı müxtəlif sahələrdə əhəmiyyətli dərəcədə dəyişməkdədir. Robot texnologiyasının və süni intellektin həyatımıza daxil olması, dövlətlərin idarəetmə sistemində özünə geniş yer alması müsbət məqamlarla bərabər, həm də ciddi problemləri qarşıya qoyur. Başqa sözlə, informasiya texnologiyalarının sürətli inkişafı, telekommunikasiya sistemlərinin imkanlarının artması kiberməkanda yeni çağırışların və təhdidlərin yaranmasına səbəb olur. Hazırda biz özəl korporativ, eləcə də ictimai maraqların geniş spektrinə təsir edən informasiya təhlükəsizliyi insidentlərinin sayında orta illik əhəmiyyətli

artımı qeyd edə bilərik. Mövcud vəziyyət informasiya təhlükəsizliyi sistemində kibertəhlükəsizliyin əhəmiyyətinin artmasını nəzərdə tutur. Kibertəhlükəsizlik sahəsinə aid olan "kiberməkan", "kibertəhlükə", "kiber təhdid" "kiberhücum" kimi əsas terminlər bir çox cəhətdən "informasiya təhlükəsizliyi", "informasiya məkanı", "informasiya təhlükəsi" terminlərinə bənzəyir. Hətta bir çox hallarda "kibertəhlükəsizlik" termini elmi ədəbiyyatda az rast gəlindiyindən, adətən, "kibertəhlükəsizlik" əvəzinə, mənaca ona yaxın olan "informasiya təhlükəsizliyi" termini istifadə edilir. Lakin "informasiya təhlükəsizliyi" daha geniş anlayışdır, "kibertəhlükəsizlik" onun tərkib hissəsi olaraq yalnız kibermühitdə olan informasiyanı əhatə edir. Başqa sözlə, "kibertəhlükə" termini "informasiya təhlükəsizliyi təhdidi" anlayışı ilə sinonim olmaqla informasiya təhlükəsizliyi kontekstində istifadə olunur. Belə yanaşma ilə "kibertəhlükəsizlik" və "informasiya təhlükəsizliyi" anlayışları arasındakı əlaqəni nəzərə almaq vacibdir, istənilən kibertəhlükə informasiya təhlükəsizliyinə təhdid olacaq, lakin informasiya təhlükəsizliyinə hər bir təhlükə kibertəhlükə olmayacaq.

Digər tərəfdən ölkələrin milli təhlükəsizlik strategiyalarında "kibertəhlükəsizlik" terminə və digər əsas terminlərə verilən təriflər də xeyli fərqlənir, hətta beynəlxalq səviyyədə də kibertəhlükəsizliyin razılaşdırılmış tam dolğun tərifi də mövcud deyil. Deməli, nəticə etibarilə kibertəhlükəsizlik strategiyalarının işlənilməsinə yanaşmalar da bu baxımdan müxtəlifdir [5]. Bunu nəzərə alaraq, məqalənin bu bölməsində "kibertəhlükəsizlik" anlayışına yanaşmalar analiz edilir və burdan irəli gələn digər anlayışların mahiyyəti və məzmunu izah olunur.

Qərbdilli ədəbiyyatda isə bu terminin birmənalı tərifi yoxdur. İngilis dilində "kiber" sözü ilə başlayan çoxlu terminlərə rast gəlmək mümkündür: kibertəhlükəsizlik, kiberfəza, kiberhücum, kibertəhdid, kibersilah, kibermüharibə, kibermühafizə və s. Belə ki, "kiber" sözü "kibernetika" sözündən törəmə olmaqla yunan dilində "kibernetes" sözündən yaranıb, mənası sükançı, idarə edən deməkdir.

Mənbələrə istinad etsək, belə qərar gələrik ki, bu termin ilk dəfə qədim yunan filosofu Platon tərəfindən işlədilib. XIX əsrdə bu söz A.Amper tərəfindən və ondan sonra bəzi Avropa müəllifləri tərəfindən işlədilmişdir. "Kibernetika" termini 1948-ci ildə amerikan alimi N.Vinerin "Kibernetika" kitabı çap olunduqdan sonra geniş yayılmağa başladı. Viner metodoloji ortaqlığı əsas götürərək kommunikasiya və idarəetməyə aid müxtəlif elmlərin bir ad altında birləşdirilməsi üçün "kibernetika" terminini işlətmişdi. "Kiberməkan" konsepti isə ilk dəfə 1980-ci illərin əvvəllərində elmi fantastika romanları ilə tanınan Uilyam Gibson tərəfindən istifadə edilmişdir [4]. Birləşmiş Krallığın kibertəhlükəsizlik strategiyası sənədində kiberməkan -"informasiyanın saxlanmasına, təşkilinə və mübadiləsinə imkan verən infrastruktur və sənaye sistemlərini, o cümlədən kompüterlər, internet və digər sistemləri dəstəkləyən

rəqəmsal və interaktiv əlaqələr şəbəkəsi kimi başa düşülür" [3].

Müasir təriflərə görə, kibernetika canlı orqanizmlər və texniki qurğular da daxil olmaqla mürəkkəb sistemlərdə idarəetmə və kommunikasiya proseslərini öyrənir [10]. Beynəlxalq Telekommunikasiya İttifaqı [11] kibertəhlükəsizliyi – "kiber mühitin aktivlərini qorumaq üçün istifadə edilə bilən alətlər, siyasətlər, təhlükəsizlik konsepsiyaları, təhlükəsizlik təlimatları, risklərin idarə edilməsi ilə bağlı yanaşmalar, tədbirlər, qabaqcıl təcrübələr, təminatlar və texnologiyalar toplusu" kimi müəyyən edir.

Daha sonra internet texnologiyalarının inkişafı ilə "kiber" əsaslı yeni sözlər yaranmağa başladı və hazırda bu sözlərdə "kiber" sözü "İnternet və virtual reallığa aid olan" mənasında işlədilir. "Kibertəhlükəsizlik" kiberfəzada informasiyanın konfidensiallığının, tamlığının və əlyetənliyinin təmin edilməsi kimi müəyyən edilir [6].

Kibertəhlükəsizlik kiberməkanda təmin edilən təhlükəsizlik kimi düşünülə bilər. Kiberməkan fiziki avadanlıq tərəfindən yaradılan və yerləşdirilən sahə olsa da, konkret sahə deyil. Kiberməkan təkcə internetlə mövcud olan məkan deyil, internetə və ya müxtəlif şəbəkələrə qoşulmayan kompüterlər də kiberməkan yarada bilər. Kiberməkan da birdən çox mücərrəd fenomendən ibarət ola bilər. Proqram təminatı, informasiya və şəbəkələr nümunə kimi göstərilə bilər [1].

Kibertəhlükəsiz anlayışlarından biri də "kiberhücum"dur. Kiberhücumlar əsasən insan tərəfindən törədilən hərəkətlərdir. İstifadə olunan alətlər və hədəf nöqtələr virtual mühit və məlumatlardan ibarət olsa da, hücumların nəticələri insanlara təsir edir və onların məqsədləri insanların yaratdığı hədəflərə əsaslanır. Kiberhücumlar klassik hakerlər, muzdlu hakerlər, daxili qüvvələr və milli dövlətlər tərəfindən həyata keçirilə bilər. Kiberhücumlar məlumatı oğurlamaq, dəyişdirmək və ya məhv etmək üçün məlumatları ehtiva edən virtual şəbəkələrə qarşı edilə bilər. Bu hücumlar cihazların və ya onlarda olan məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını məhv etmək üçün kompüterdən kompüterə həyata keçirilir [7].

Kiberhücumun vurduğu zərər üç dərəcədir. İlk növbədə kiberhücum kompüter sistemləri və ya şəbəkələri, verilənlər, proqram təminatı və ya sistemləri hədəf alır. Ona görə də kiberhücum bilavasitə kiber aləmə ziyan vurur. Ancaq kiber mühitdəki hücum birbaşa kompüter sistemlərinə təsir etsə də, sistemdə meydana gələn zərər istifadə olunduğu xidmətlərə və nəhayət, kompüter sistemlərinin bu xidmətdən faydalanan şəxslərə təsir edir. Nəticədə kiberhücumlar domino effekti yaradır və təkcə kompüter sistemlərinə deyil, həm də kompüter sisteminin təqdim etdiyi xidmətlərə və əlaqədar xidmətlərdən faydalanan şəxslərə zərər verir [8, s.53-53].

Ümumilikdə "kibertəhlükəsizlik", "kibertəhlükə" və "kibertəhdid" terminləri kiberməkanın komponentlərinin təhlükəsizliyi kontekstində istifadə oluna bilər. Məsələn, bir çox tədqiqatçılar və mütəxəssislər hərbi məqsədlər üçün avtomatlaşdırılmış idarəetmə sistemlərinin kibertəhlükəsizliyi dedikdə, saxlanılan,

emal edilən və hərbi avtomatlaşdırılmış idarəetmə sistemlərinə ötürülən məlumatların informasiya-texniki xarakterli təhlükələrdən qorunmanın vəziyyəti başa düşülür. "Kibertəhlükə" termini məlumat və ya avtomatlaşdırılmış idarəetmə sisteminin, onun obyektlərinin və ya iş mühitinin vəziyyətinə məlumat və texniki təsirləri müəyyən edən, yolverilməz zərərə və ya idarəetmənin qeyri-mümkünlüyünə səbəb ola biləcək şərtlər və amillərin məcmusu kimi izah edilir. Bu cür yanaşma kiberməkanın bütün komponentlərinin kibertəhlükəsizliyini nəzərə almaq üçün istifadə edilə bilər [9, s.30].

Beləliklə, elmi ictimaiyyətdə "kiberməkan", "kibertəhlükəsizlik", "kibertəhlükə" və "kibertəhdid" və "kiberhücum" terminlərinin vahid tərifi olmadığından, bu terminlərin tərifinə baxılan yanaşmalardan hər hansı birini ayrıca qeyd etmək mümkün deyil. Amma daha konkret və yığcam şəkildə bu anlayışların mahiyyətini əks etdirəcək aşağıdakı formullardan istifadə etmək olar. Kiberməkan – praktiki olaraq qeyri-məhdud miqdarda məlumatı özündə birləşdirən bir-biri ilə əlaqəli kompüterlər şəbəkəsi tərəfindən yaradılmış məkandır; kibertəhlükəsizlik – təhlükə və təhdidlərin minimuma endirildiyi kiberməkanın vəziyyətinin arzuolunan məqsədi; kibertəhlükə – siyasi, sosial və ya digər məqsədlərə nail olmaq üçün virtual məkana qeyri-qanuni zərərli nüfuzetmə yolu ilə kibertəhlükəsizliyin pozulmasının real mümkünlüyü ilə xarakterizə olunan şərtlər və amillər məcmusu; kibertəhdid – müəyyən şəraitdə kibertəhlükənin yaranmasına səbəb ola biləcək şərtlər və amillərin məcmusudur. Kiberhücum – gizli məlumatlara giriş əldə etmək, onu dəyişdirmək, məhv etmək, istifadəçilərdən vəsait əldə etmək, təşkilat və ya şirkətlərin normal fəaliyyətini pozmaq məqsədilə həyata keçirilir.

Ümumilikdə isə kibertəhlükəsizlik dedikdə, sistemlərin, şəbəkələrin və proqram təminatlarının rəqəmsal hücumlardan, təhlükələrdən, təhdidlərdən qorunması üçün tədbirlərin həyata keçirilməsi, sistemin sabitliyinin, dayanıqlığının və təhlükəsizliyinin təmin olunması və baş verə biləcək hadisələrin aradan qaldırılmasıdır.

2. Kiberhücumlara qarşı mübarizədə dövlətlərin davranışları.

Qloballaşmanın və informasiya texnologiyalarının, internetin durmadan inkişafı və dövlət idarəçiliyi, bank, nəqliyyat və digər sahələri əhatə edir. Texnoloji məhsulların köməyi ilə hər gün daha çox məlumat və sənədlər verilənlər bazalarına köçürülür, orada saxlanılır, təhlil edilir və istifadə olunur. Əslində bu məlumatlar lazım gəldikdə asanlıqla bir yerdən başqa yerə köçürülür. Buna uyğun olaraq, inkişaf edən informasiya texnologiyaları çərçivəsində ölkələr tərəfindən vətəndaşlara təklif olunan bir çox xidmətlər internet üzərindən həyata keçirilir. Bu sistemlər enerji nəqli və rabitə kimi mühüm infrastruktur sektorlarında, eləcə də dövlət qurumlarında geniş istifadə olunur. Bu sistemlər həm göstərilən xidmətlərin keyfiyyətinə, həm də müvafiq qurumun/təşkilatın daha səmərəli fəaliyyətinə töhfə verir.

Amma unutmaq olmaz ki, qeyd olunan sahələrin inkişafı və daha

səmərəli, effektiv fəaliyyəti üçün mütləq halda tətbiq edilən innovativ yeniliklər, smart texnologiyalar başqa bir tərəfdən kibercinayətkarlığın meydana gəlməsinə və gündən-günə artmasına səbəb olur. Çünki qurum və təşkilatların məsuliyyəti altında olan məlumatların tam təhlükəsizliklə qorunması zəruridir və qeyd olunan sistemlərin təhlükəsizliyinin təmin edilməsi milli təhlükəsizlik baxımından böyük əhəmiyyət kəsb edir. Bu cür sistemlərin təhlükəsizliyi təmin edilmədikdə isə zərərli proqramlar, fişinq, hədəflənmiş hücumlar və s. kimi təhdidlər milli təhlükəsizlik risklərinə, insan tələfatı, ictimai asayişin pozulmasına və s. halların baş verməsinə gətirib çıxara bilər.

Görünən odur ki, qeyd olunan məsələlərin həlli hazırkı dövrdə dövlətlərin milli təhlükəsizliyi qarşısında mühüm prioritet istiqamət kimi dayanır və milli təhlükəsizlik sisteminin təkmilləşdirilməsini, kibermüdafiə tədbirlərinin genişləndirilməsini vacib edir. Habelə kibertəhlükəsizliyin: kiberhücumun, kibertəhdidin qarşısının alınması və təhlükəsizliyin təmin olunması üçün preventiv tədbirlərin görülməsini aktuallaşdır.

Məhz bu səbəbdən 2007-ci ildə Estoniya, 2008-ci ildə Gürcüstan və 2010-cu ildə İrana qarşı dövlət tərəfindən maliyyələşdirildiyi iddia edilən kiberhücumlar, kibertəhlükəsizliyin milli və beynəlxalq təhlükəsizlik məsələsinə çevrilməsində mühüm rol oynamış oldu. Şimali Atlantika Müqaviləsi Təşkilatı (NATO) Estoniyadakı hücumdan dərhal sonra Estoniyanın paytaxtı Tallində və 2016-cı ildə Varşava Sammitində kiberməkanda Mükəmməl Kiber Müdafiə Mərkəzi yaratdı.

Beləliklə, NATO kiberhücumları da yaxşı əhatə edən kibermüdafiə strategiyası hazırlayarkən üzv dövlətlər kiberhücumla mübarizə apara biləcək bölmələr yaratmağa başladılar. Hazırda 100-dən çox dövlət öz kiber imkanlarını müəyyən etmiş və 50-dən çoxu öz milli kiberstrategiyalarını müəyyənləşdirmişdir [2, s.16-17].

Kiberdiplomatiya kiberməkanın militarizasiyasından geri qalsa da, son illərdə qlobal kibernormaların qəbulu üçün bir çox beynəlxalq təşəbbüslərlə çıxış etmişdir. Kiber normaların yaranması və kiberməkanla bağlı beynəlxalq rejimlərin formalaşması beynəlxalq hüququn kiber məkanda dövlətin davranışlarına rəhbərlik etməli olduğunu açıq şəkildə göstərmiş oldu. Birləşmiş Millətlər Təşkilatının (BMT) tərksilah və beynəlxalq təhlükəsizlik məsələləri ilə məşğul olan Birinci Komitəsi bu müzakirələr üçün ilkin və vacib forumlardan biri olmuşdur. 1999-cu ildən bəri Birinci Komitə nəzdində aparılan danışıqlarda BMT-yə üzv dövlətlər beynəlxalq hüququn kiberməkana tətbiqi, sülh dövründə dövlətlərin məsuliyyətli davranış normalarını müəyyən etmişlər. Danışıqlar zamanı kiber hadisələr nəticəsində yaranan münaqişə riskini azaltmağa kömək etmək üçün etimadın möhkəmləndirilməsi tədbirləri və inkişaf etməkdə olan ölkələrin kiberhücumlara effektiv cavab verməsi üçün potensialın gücləndirilməsi üzərində qurulmuş beynəlxalq çərçivə ətrafında getdikcə daha çox birləşməyin

vacibliyi qərara alınmışdır.

Heç şübhəsiz ki, dövlətlərin kibertəhlükəsizliklə bağlı narahatlığı və buna uyğun preventiv tədbirlər görmək istəkləri və atdıqları addımlar təsadüfi deyil. Çünki kiberhücumlar hədəf aldıqları qrupa və istifadə etdikləri üsullara görə terror fəaliyyətləri ilə yanaşı, maddi hücumların da mövzusu ola bilir. Əslində bəzi terror təşkilatlarının və ya mütəşəkkil cinayətkar təşkilatların dövlətin müəyyən vahidlərinə kiberhücumlar həyata keçirməsi, kiberhücumların getdikcə klassik terror fəaliyyətini əvəzləməsi hadisələri baş verir.

Klassik terror fəaliyyətlərindən fərqli olaraq, kiberhücumlarda iştirak edən fərdlərin və qrupların kimliyi məxfidir və kiberməkanda aşkarlanması çətindir. Həm kibercinayətlər, həm də kibercinayətlərdən daha ağır olan kiberhücumlar kiberhücumun başladığı və təsirləndiyi yerə, hücumu həyata keçirən və hücumdan təsirlənən insanlara görə beynəlxalq ictimaiyyətlə sıx bağlıdır.

Bu səbəbdən qlobal miqyasda kibertəhlükəsizliyin yaradılması üçün lazımi tədbirlər beynəlxalq hüququn əhatə dairəsinə düşür. Amerika Birləşmiş Ştatları, Avstraliya, Çin, Kuba, Macarıstan, İran, İtaliya, Mali, Hollandiya, Qətər, Rusiya Federasiyası, Böyük Britaniya kimi dövlətlər və Avropa İttifaqı kimi beynəlxalq təşkilatlar kiber fəaliyyət baxımından gücdən istifadənin qadağan edilməsini lazım bilirlər. Bunun əks effektlərə səbəb olacaqlarından ehtiyat edirlər. Əvəzində kibercinayətkarlığın kiberhücum səviyyəsinə çatdığı hallarda kibertəhlükəsizliyin təmin edilməsi məqsədilə kiberhücumların qarşısının alınması və kiberterrorizmlə mübarizə məqsədi ilə beynəlxalq sülh və təhlükəsizliyin təmin edilməsi üçün beynəlxalq hüququn tətbiq etdiyi ümumi qayda və mexanizmlərin həyata keçirilməsini daha doğru hesab edirlər. Habelə, problemin qarşısının alınmasında müasir texnologiyalardan düzgün və səmərəli istifadəsinin effektivliyinə də inanırlar.

Amma bu o demək deyil ki, kiberhücumlara qarşı mübarizədə gücdən istifadə heç bir halda mümkün deyil. Kiberhücum güc tətbiqi qadağası çərçivəsində olarsa və hətta silahlı hücuma səbəb olarsa, beynəlxalq ictimaiyyətin silahlı hücuma qarşı görəcəyi tədbirlər də dəyişir. Kiberhücumun hüquqi mahiyyətinə uyğun olaraq kiberhücum klassik mənada hücumun əhatə dairəsinə düşə bilər. Bu halda hücuma məruz qalan dövlət əks tədbirlər görə biləcək və dövlətin məsuliyyəti ilə bağlı qaydalara uyğun olaraq dəymiş ziyan ödənilə bilər.

Kiberhücumun silahlı hücum səviyyəsinə çatması halında kiberhücuma məruz qalan dövlətin özünümüdafiə hüququ yaranacaq. Klassik özünümüdafiədə olduğu kimi, kiberhücuma qarşı özünümüdafiə hüququ zəruri, təmkinli və təcili olmalıdır. Burada ən mühüm məsələ, fikrimizcə, mötədilliklə bağlıdır. Beynəlxalq hüquqda bəzi müəlliflər kiberhücuma qarşı istifadə oluna biləcək özünümüdafiəni kiberməkanda məhdudlaşdırmağın daha məqsədəuyğun olduğunu iddia edirlər. Nəticədə, kiberhücumlara qarşı istifadə edilən özünümüdafiə hüququ, istər kiberməkanda, istərsə də fiziki mühitdə, son nəticədə

ölçülməlidir.

Hesab edirəm ki, gücdən istifadənin qadağan edilməsinin əksinə olaraq, beynəlxalq sülh və təhlükəsizliyin qorunması üçün bu qadağanın yeganə istisnası olan özünümüdafiə hüququnun mümkün qədər dar çərçivədə şərh edilməsi çox vacibdir. Bu baxımdan, fikrimizcə, müvafiq yanaşma təkcə maddi dünyada deyil, həm də kiber aləmdə keçərli olmalıdır. Əslində kiber dünyada özünümüdafiə hüququndan istifadə daha da məhdudlaşdırılmalıdır, çünki hücumun silahlı hücuma keçib-keçmədiyini müəyyən etmək çox çətindir və hücumun mənbəyini müəyyən edib hər hansı dövlətə aid etmək çox çətindir. Odur ki, özünümüdafiə hüququnun həyata keçirilməsi üçün kiberhücum dövlət və ya qeyri-dövlət qrupu və ya dövlətlə möhkəm əlaqələri olan şəxslər tərəfindən həyata keçirilməlidir. Aydındır ki, özünümüdafiə hüququ dövlət tərəfindən dəstəklənməyən qruplar və terror təşkilatları tərəfindən həyata keçirilən kiberhücumlara qarşı mübarizədə istifadə edilə bilməz. Hazırkı dövrdə bu terrorçular üçün geniş imkanlar açа bilər. Necə ki, terrorçular əsasən kiberhücumlardan istifadə etməklə dövlətləri təhdid edir və ya ciddi aktlar törədirlər.

Bu halda ən effektiv yol, dövlətlərlərin birgə fəaliyyəti, problemlə sistemli yanaşması və beynəlxalq hüquq norma və prinsiplərinin üstün tutulması vacibdir. Əsasən də problemə BMT sistemi çərçivəsində həll variantının tapılması mütləqdir. Amma məsələyə təkcə böyük olan dövlətlərin təhlükəsizlik maraqları çərçivəsində deyil, bütün dövlətlərin maraqları çərçivəsində baxılması mütləqdir. Əks təqdirdə hətta böyük dövlətlərin belə kiberhücumlardan tam olaraq qorunmasından danışmaq olmaz. Başqa sözlə, kiberhücumun heç bir dövlətlə əlaqələndirilməsi mümkün olmasa belə, kiber mühitdə beynəlxalq sülhü təhdid edən və ya pozan bir fəaliyyətin və ya kiberhücum vəziyyətinin BMT Təhlükəsizlik Şurası tərəfindən aşkarlanması mümkün ola bilər. Kiberhücumun qarşısını almaq üçün lazımi tədbirlər görməyən və əməkdaşlıq etməyən, hətta bu cür amillərdən digər dövlətlərə qarşı mübarizə vasitəsi kimi istifadəyə cəhd edən dövlət üçün bu vəziyyət beynəlxalq öhdəliyin pozulması anlamına gəlir və bu vəziyyət həmin dövlətin beynəlxalq məsuliyyətini ortaya çıxarır.

Beləliklə, kibertəhlükəsizliyin təmini, kiberhücumlardan müdafiə daha çox dövlətlərin birgə fəaliyyəti, qarşılqılı əməkdaşlığı, səylərin birləşdirilməsi və beynəlxalq hüquqa hörmət prinsiplərindən asılıdır.

Nəticə

Kibertəhlükəsizlik kiberfəzada informasiyanın konfidensiallığının, tamlığının və əlyetənliyinin təmin edilməsi kimi müəyyən edilir. Kompüterlərə və oxşar şəbəkələrə və ya sistemlərə qarşı aqressiv fəaliyyət və kritik kiber sistemləri, aktivləri və funksiyaları pozmaq və ya tamamilə məhv etmək kiberhücumların əsas hədəfləridir. Ayrılıqda fərdin, qrupun kiberhücumların hədəfi olsalar da, amma müasir dünyamızda əsas hədəf kimi dövlətin özü daha

çox gündəmə gətirir. Çünki hazırkı münaqişə və müharibələri hibrid müharibələr kimi xarakterizə etmiş olsaq, bu vasitə getdikcə daha çox istifadə edilir.

Nəzərə alsaq ki, kiberməkan hazırkı dövrdə dövlət idarəçiliyini, bank, maliyyə, nəqliyyat və digər bir çox vacib sahələri əhatə edir, deməli, kiberhücumların, kibertəhdidlərin olması qaçılmazdır. Onu da nəzərə alaq ki, bu gün dövlətlərin bir-birinə qarşı istifadə etdikləri kiberhücumlar və ya kibertəhlükəsizliyin pozulmasına yönəlik addımlar sonrakı dövrdə onların özləri üçün ciddi problemə çevrilir. Yəni bu vəziyyət bir çox hallarda üçüncü tərəfin və ya terrorçu qrupların, kibercinayətkarların əlində bir vasitəyə çevrilməklə dövlətlərin milli təhlükəsizliyinə təhdid yaradır. Çünki kibertəhlükəsizliyin etibarlı təmin edilməsi dövlətin təkbaşına imkanları xaricindədir, bu problemin həlli bütün maraqlı tərəflərin – dövlətin, özəl sektorun və vətəndaşların tərəfdaşlığını və əməkdaşlığını tələb edir. Başqa sözlə, mövcud reallıq: informasiya cəmiyyətinin, informasiya-kommunikasiya texnologiyalarının sürətli inkişafı kibertəhlükəsizliyin təmin edilməsi istiqamətində effektiv nəticələrin əldə edilməsi üçün beynəlxalq əməkdaşlığın dərinləşdirilməsini və qarşılıqlı yardımın artırılmasını vacib edir. Bunun üçün mühüm olan istiqamətlərdən biri də dövlətlərin təhlükəsizlik doktrinalarını, strategiyalarını və qanunvericilik aktlarını hazırlayarkən kibertəhlükəsizliyin təmin edilməsi mexanizmlərini birgə nəzədən keçirmələri doğru olardı. Habelə kiberhücumlara qarşı mübarizədə müasir texnoloji imkanlardan istifadə vacibdir. Bu istiqamətdə yeni innovativ texnologiyanın tətbiqi üçün tədqiqatların, araşdırmaların aparılması zəruridir.

ƏDƏBİYYAT

1. Clark D., Berson T. and Lin H.S. At the nexus of cybersecurity and public policy. Some Basic Concepts and Issues / D. Clark, T. Berson and H.S.Lin, Washington DC: The National academies press, 2014, 50 p.
2. *Deibert R. and Rohozinski R.* Risking security: policies and paradoxes of cyberspace security // International political sociology, 2010 4 (1), pp.16-17
3. GCHQ 10 Steps to Cyber security. UK: Crown, 2012
4. *Kara M.* Siber saldırılar-siber savaşlar ve etkileri. Yayınlanmamış yüksek lisans tezi, İstanbul: Istanbul Bilgi Universitesi Sosyal Bilimler Enstitüsü, 2013
5. *Luiijf H., Besseling K. and de Graaf P.* Nineteen national cyber security strategies. International journal for critical infrastructures, 2013, 9 (1, 2)
6. *Mitra A., Schwartz R.L.* From cyber space to cybernetic space: rethinking the relationship between real and virtual spaces // Journal of computer-mediated communication, october 2001, vol. 7, No 1
7. National Cyber Security Framework Manual / ed. Alexander K. Tallinn: NATO CCD COE publication, 2012, 254 p.

8. *Roscini M.* Cyber Operations and the Use of Force in International Law / M.Roscını. Oxford University Press, 2014, pp.52-53
9. *Дзялошинский И.М.* Информационное пространство России: структура, особенности функционирования, перспективы эволюции / И. М. Дзялошинский. Москва: Центр Карнеги, 2001. 30 с.
10. *Теслер Г.С.* Новая кибернетика / Г.С.Теслер. Киев: Логос, 2004, 401 с.
11. ITU. Global cybersecurity index and cyberwellness profiles reports (GCI) aprel, 2015. 528 p. // URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

Redaksiyaya daxil olub 29.11.2022