BEYNƏLXALQ MÜNASİBƏTLƏRDƏ KİBERTƏHLÜKƏSİZLİK PROBLEMİ

UOT 327; 930.22
DOI:10.30546/3006-0346.2024.5.83.017

MƏHƏBBƏT SEYİDOVA
Bakı Dövlət Universitetinin
Beynəlxalq münasibətlər kafedrasının
doktorantı

E-mail: mahabbatseyidova78@gmail.com
https://orcid.org/0009-0000-1094-8477

Giriş

Müasir dünyada kiberməkanda edilən cinayətlərin sayı əhəmiyyətli dərəcədə artmışdır. Müntəzəm olaraq qanunsuz hədəflərin əldə edilməsi məqsədilə istifadə edilən pisniyyətli proqram tətbiqlərin yeni növləri meydana gəlir. Ekspertlərin hesablamalarına görə, informasiya-kommunikasiya texnologiyaların (İKT) köməyi ilə edilən cinayətlərin dünya iqtisadiyyatına vurduğu maddi ziyan trilyon ABŞ dolları ilə hesablanır. Bu cür miqyaslar kiberməkanda yaranan münasibətlərin effektiv hüquqi tənzimlənmə vasitələrini tələb edir. Kibertəhlükəsizlik dövlətin, milli təhlükəsizliyin təmini üçün mühüm əhəmiyyət kəsb etməkdədir. İKT iqtisadi, sosial, mədəni və siyasi münasibətlərə mənfi təsir göstərə bilər, dövlətin və cəmiyyətin iqtisadi, hərbi, müdafiə potensialına ziyan vura bilər. Buna görə də beynəlxalq ictimaiyyət kibertəhlükəsizlik sahəsində əməkdaşlığın çoxtərəfli hüquqi əsaslarının işlənib hazırlanmasında maraqlıdır. Lakin bu vəzifənin həlli ilə bağlı beynəlxalq səviyyədə vahid yanaşma yoxdur, belə ki, kiberməkanın hüquqi tənzimlənməsinin mürəkkəbliyi bu sahədə yaranan münasibətlərin virtual xüsusiyyətləti ilə şərtlənib.

Aparılan analiz göstərdi ki, informasiya sahəsində tətbiq olunan müasir beynəlxalq hüququn prinsip və qaydalarına baxmayaraq, kiberməkanın səciyyəvi xüsusiyyətləri və qanunsuz məqsədlər üçün istifadə olunma imkanları nəzərə alınmaqla mövcud beynəlxalq hüquq normalarının universallaşdırılması tələb olunur. Dövlətlərin kiberməkanda davranış qaydalarını tənzimləmək məqsədi daşıyan səyləri insan haqları, məlumatların məxfiliyi və s. bu kimi məsələlərlə məhdudlaşır. Heç də bütün dövlətlər kiberməkanda müasir və effektiv əməkdaşlıq mexanizminin yaradılmasında maraqlı deyillər, açıq şəkildə yeni beynəlxalq hüquq normalarının işlənib hazırlanmasına qarşı çıxış edirlər.

Məqalədə sənədlərin və praktikanın analizi əsasında göstərilir ki, kibertəhlükəsizlik dövlətin təhlükəsizliyi ilə birbaşa bağlı olan məsələdir. Kibertəhlükəsizliyin təmini probleminə dövlətlərin müxtəlif yanaşmaları bu sahədə əməkdaşlıq üçün effektiv çoxtərəfli hüquqi əsasların olmamasına səbəb olur.

Tədqiqat işində təsviri, tarixi-müqayisəli, analitik tədqiqat metodlarından istifadə edilmişdir. Tədqiqatda sistemli yanaşma, analiz, sintez metodlarına da yer verilmişdir.

Qlobal informasiyalaşma və kiberməkan. Qlobal informasiyalaşma hazırda dövlətlərin mövcudluğunu və fəaliyyətini fəal şəkildə idarə edir, informasiya texnologiyaları milli, hərbi, iqtisadi təhlükəsizliyin təmin edilməsi məsələlərinə tətbiq edilir. Bundan başqa, dövlət və hərbi strukturların qlobal informasiyalaşdırmalarının fundamental nəticələrindən biri rəqib dövlətlər üçün yeni qarşıdurma sahəsi olan coğrafi sərhədləri olmayan, lakin beynəlxalq olan kiberməkanın yaradılması oldu. Əgər bu gün hərbi və iqtisadi münasibətlərdə aparıcı olan dünya ölkələri arasında adi və kütləvi qırğın silahlarının tətbiqi sahəsində müəyyən paritet yaranıbsa və yerüstü, dəniz, hava, kosmik məkanlarda dövlətlər arasında qarşılıqlı əlaqələrin əsas prinsipləri formalaşıbsa, kiberməkanda dövlətlərarası paritet və qarşılıqlı münasibətlər məsələsi açıq olaraq qalmaqdadır.

Qlobal kiberməkanın yaranma prosesində hərbi və mülki kompüter texnologiyalarının konvergensiyası baş verir, aparıcı xarici ölkələrlə potensial rəqiblərin informasiya infrastrukturuna yeni fəal təsir üsulları və metodları intensiv şəkildə işlənib hazırlanır, əsas vəzifəsi dövlət və hərbi informasiya infrastrukturların müdafiəsi, rəqib informasiya sistemlərində fəal destruktiv hərəkətlərin hazırlanması və aparılması olan müxtəlif ixtisaslaşdırılmış kibernetika mərkəzləri, idarəetmə orqanları yaradılır. ABŞ, Çin, Böyük Britaniya, Fransa, Almaniya, İsrail və başqa dövlətlər artıq şəxsi rəsmi kiberqoşunlara malikdirlər.

Kiberməkanda qarşıdurma dövlətlər arasında prinsip etibarilə yeni qarşıdurma sahəsinə çevrilir. "Kiber..." başlığı ilə terminlər və anlayışlar beynəlxalq və dövlətdaxili müzakirələrdə və sənədlərdə geniş istifadə olunur, bir sıra dövlətlərin və NATO daxil olmaqla beynəlxalq təşkilatların strateji doktrinalarında öz əksini tapır. Kiberməkan probleminə dünyada artan maraq daha çox ABŞ-nin kibermüharibələr və kibertəhlükəsizlik məsələlərindəki fəallığı ilə əlaqədardır.

Texnoloji və hərbi liderliyini qoruyub saxlayan ABŞ-da kiberməkanda siyasi və hərbi fəaliyyəti tənzimləyən bir sıra direktivlər və rəsmi sənədlər yüksək səviyyədə qəbul edilmişdir. Nümunə olaraq, "Kiberməkanda siyasətin icmalı"(may, 2009-cu il) [1,3], "Kiberməkan üzrə beynəlxalq strategiya" (may, 2011-ci il)[2,4], "Müdafiə nazirliyinin 2011-ci il kiberməkanda fəaliyyət strategiyası"(iyul, 2011-ci il) [3, 6] adlı sənədləri göstərmək olar. Sonuncu sənədin təqdimatı zamanı müdafiə nazirinin müavini Uilyam Linn qeyd etmişdir ki, "XXI əsrdə bitlər və baytlar güllələr və bombalar kimi təhlükəli olacaqlar. Strategiyanın mahiyyəti ondan ibarət idi ki, kiberməkan rəsmi Vaşinqton tərəfindən yer, hava, dəniz və kosmos kimi potensial döyüş meydanı kimi baxılır. Ona görə də ABŞ kiberhücum aktlarını ənənəvi hərbi əməliyyatlara bərabər tutur və "ciddi hücumlara proporsional və ədalətli hərbi tədbirlər ilə (nüvə silahı da daxil olmaqla) cavab vermək" imkanını nəzərdə tuturlar. Eyni zamanda Pentaqon nümayəndələri qeyd edirlər ki, bu doktrina kiberməkanda ilk addımdır və gələcəkdə müdafiə siyasətindən təhdidlərin qarşısının alınması siyasətinin və mümkün hücum tədbirlərinin işlənməsinə keçmək olar.

Strateji sənədlərində Pentaqon kiberməkanı mümkün hərbi əməliyyatların yeni meydanı kimi qəbul edir, NATO alyansının üzv-dövlətlərində qarşı kiberhücumları silahlı hücuma bərabər tutur. İnkişaf etmiş dövlətlərin (ABŞ, NATO blokunun üzv-dövlətləri, Yaponiya, Çin və b.) informasiya texnologiyaları üzrə mütəxəssisləri yekdilliklə bir faktı qeyd edirlər ki, "kiberməkana nəzarət edən dövlətlər sülh və müharibəyə də nəzarət edəcəklər".

Kibertəhlükəsizlik və kibermüharibə. Kibertəhlükəsizlik dövlət əhəmiyyətli strateji problem olub, cəmiyyətin bütün təbəqələrini əhatə edir. Kibertəhlükəsizlik üzrə dövlət siyasəti dövlətlərin informasiya sistemlərinin təhlükəsizliyini və etibarlılığını gücləndirmək məqsədi dayışır. ABŞ-nin ardınca kibertəhlükəsizlik strategiyaları Kanada, Yaponiya, Hindistan, Yeni Zelandiya, Kolumbiya və bir sıra başqa ölkələrdə qəbul edilib. Avropa İttifaqına daxil olan İsveç (2008-ci il), Estoniya (2008-ci il), Finlandiya (2008-ci il), Slovakiya (2008-ci il), Çexiya (2011-ci il), Fransa (2011-ci il), Almaniya (2011-ci il), Litva (2011-ci il), Lüksemburq (2011-ci il), Hollandiya (2011-ci il), Böyük Britaniya (2011-ci il) kimi ölkələrdə də kibertəhlükəsizlik strategiyası qəbul edilib. Ölkələrin siyahısı aydın şəkildə göstərir ki, kibertəhlükəsizlik problemi dünyada vacib hesab edilir.

2008-ci ildən NATO informasiya təhlükəsizliyi sahəsində illik kibertəlimlər keçirir. 2013-cü ilin aprelində təşkil edilən "Locked Shields-2013" adlı təlimlərdə kompüter şəbəkələrinə kiberhücumların dəf edilməsi ilə bağlı təlimlər keçirilmişdir. Təlimlərdə 9 ölkədən 250-ə yaxın mütəxəssis iştirak etmişdir: Estoniya, Finlandiya, Litva, Almaniya, Polşa, Hollandiya, İtaliya, Slovakiya, İspaniya.

ABŞ-nin Milli Təhlükəsizlik Nazirliyinin kadrlarının hazırlıq səviyyəsinin artırılması çərçivəsində ölkənin mülki kolleclərində və hərbi akademiyalarında təhsil alanlar üçün hər il "Kiber Müdafiə Təlimi" ("Cyber Defense Exercise") keçirilir. Təlimlərdə əsas məqsəd amerikalı hərbi qulluqçularda informasiya texnologiyaları sahəsinə marağı və onların bilgilərini artırmaqdır.

Şəbəkə və informasiya təhlükəsizliyi üzrə Avropa Agentliyi (European Network and Information Security Agency, ENISA) dövlət və özəl sektor təşkilatlarının kiberhücumları dəf etmək məqsədilə 2012-ci ilin oktyabrında "Avropa kiber təlimi" (European Cyber Exercise) adlı kibertəlimlər keçirmişdir.

ABŞ-nin keçmiş prezidenti Barak Obamanın dövründə bu problemin beynəlxalq-müqavilə aspektlərinə artan diqqət göstərilməyə başlandı.Vaşinqtonun kibermüharibələr və kibertəhlükəsizlik məsələlərində fəallığı bu problemə beynəlxalq marağı kəskin şəkildə artırdı. Kibertəhlükəsizlik dünya mediasında, beynəlxalq tədbirlərdə müzakirə olunan aktual siyasi problemlərdən birinə çevrildi. Təhlükəsizlik texnologiyaları ilə məşğul olan "McAfee" şirkətinin "Virtual cinayətkarlıq haqqında illik hesabatı"nda birmənalı olaraq qeyd edilir ki, "kibersilahlanma uğrunda beynəlxalq yarış reallığa çevrilib", siyasi maraqlardan irəli gələn kiberhücumların dünyada sayı artıb, bir sıra ölkələr kibersilaha malikdirlər və ya onun hazırlanması ilə məşğuldurlar. ABŞ-nin informasiya təhlükəsizliyi sahəsindəki ekspertlərinin hesablamalarına görə, hazırda bu kimi dövlətlərin sayı 30-dan artıqdır.

ABŞ Kibernetka komandanlığının rəhbəri, general Kit Aleksander 2013-cü ilin iyununda Tallində keçirilən NATO-nun kibermüdafiə ilə bağlı konfransında çıxışı zamanı ilk dəfə olaraq etiraf etdi ki, kiberməkanda insidentlər "dövlətlər arasında genişmiqyaslı hərbi münaqişələrə səbəb ola bilər". BMT-nin Beynəlxalq Telekommunikasiya İttifaqının baş katibi Xamadun Ture bildirdi ki, "növbəti dünya müharibəsi baş verdiyi təqdirdə kiberməkanda cərəyan edəcək".

Müasir şərtlərdə XXI əsr müharibələrinin mahiyyət etibarilə kibermüharibələr olacağını bəyan etmək ədalətli mövqedir. Nəticə etibarilə, hər bir dövlət üçün kiberməkanda təhlükəsizlik (kibertəhlükəsizlik) öz milli təhlükəsizliyinin təmini və maraqlarının qorunmasında kəskin və spesifik problemə çevrilir.

"Kibertəhlükəsizlik" termini həyatımıza kompüter və kompüter sistemlərinin yaranma anından daxil olub və nəticədə cəmiyyət həyatın qızğın, miqyaslı və əhəmiyyətli informasiyalaşmasının girovuna çevrilib və gündəlik fəaliyyət, ekologiya, sağlamlıq, geniş mənada mövcudluğu ondan asılı hala düşüb. Müasir şərtlərdə "kibertəhlükəsizlik" məsələləri adi hesablayıcı texnikada informasiyanın müdafiəsi səviyyəsindən informasiya və milli təhlükəsizliyin tərkib hissəsi olaraq dövlətin vahid "kibertəhlükəsizlik" sisteminin yaradılması səviyyəsinə qədər qalxır və bütün kiberməkanın müdafiəsinə görə məsuliyyət daşıyır.

Dövlət və hərbi idarəetmə sistemlərində kibertəhlükəsizliyin təmin edilməsi probleminin düzgün formalaşması və həlli məqsədilə, ilk növbədə, kibertəhlükəsizlik probleminin milli, hərbi, informasiya təhlükəsizliyi və texnoloji müstəqillik problemlərinin sırasında yerini və rolunu müəyyən etmək lazımdır.

Bu gün kiberməkanla bağlı beynəlxalq ictimaiyyətin yekdil olaraq qəbul etdiyi bir tərif yoxdur, lakin çoxlu sayda şəxsi anlayışlar mövcuddur. İstifadə olunan anlayışlar kiberməkanın hansı baxış bucağından baxılmasından asılı olur – dövlətin informasiya-kommunikasiya infrastrukturunun müdafiəsinin təmini nöqteyi-nəzərindən, yaxud kiberməkan fəal hərbi əməliyyatların aparılması nöqteyi-nəzərdən.

Bundan başqa, beynəlxalq hüquqda "kiberməkan", "kibermüharibə", "kiberhücum", "kiberterrorizm", "kiberfəlakət", "kibertəhlükəsizlik" və s. anlayışlarla bağlı konsensusun olmaması dövlətlər arasında bu sahədə əlaqələrin qurulumasında mənfi faktor hesab edilir.

Kiberməkanın ümumdövlət tərifi ilk dəfə olaraq ABŞ Konqresinin tədqiqat xidmətinin 2001-ci il hesabatında qeyd edilib və bildirilib ki, kiberməkan "fiziki coğrafiyadan asılı olmayaraq kompüterlər və telekommunikasiyalar əsasında insanlar arasında yaradılan çoxsaylı hərtərəfli əlaqələr" kimi təyin edilib.

2001-ci ildən başlayaraq ABŞ Müdafiə Nazirliyinin müxtəlif nizamnamə sənədlərində "kiberməkan" anlayışının transformasiyası baş verirdi. Amerika hərbi rəhbərliyin kiberməkanda mübarizə sahəsində anlayışların yaranmasına baxış və yanaşmalarının təkamülü hərbi-strateji vəziyyətin dəyişmiş xarakterini və informasiya və kompüter texnologiyalarının silahlı qüvvələrin fəaliyyət sahəsinə dərin nüfuzunu nəzərə alaraq hərbi sənətin əsas müddəalarına yenidən baxılması faktını təsdiq edir. Eyni zamanda ekspert səviyyəsində kiberməkanda hərbi əməliyyatların aparılması nəzəriyyəsi üzərində iş gedir və onun uğuru vaxtında yaradılacaq texnoloji ehtiyatdan, kiber qarşıdurmanın müvafiq üsul və formalarının mənimsənilməsindən asılı olacaq.

Kiberməkanda əməliyyatlar aparmaq və bu sahə vasitəsilə dünya proseslərinə təsir göstərmək məqsədilə "kibersilahlanma" sistemi (kibervasitələrin, infrastrukturun və kadr ehtiyatlarının təşkilati-funksional birlik sistemi) yaradılır.

Kibertəhlükəsizlik sahəsində standart ISO/IEC 27032:2012 "İnformasiya texnologiyaları. Təhlükəsizliyin təmini üsulları. "Kibertəhlükəsizliyin" təmini üzrə rəhbər göstərişlər" kiberməkanı "kompleks mühit və insanlar, proqram təminatı və İnternətə qoşulan və fiziki formada mövcud olmayan texnoloji qurğular və şəbəkənin köməyilə İnternetdə xidmətlər arasında qarşılıqlı əlaqənin nəticəsi" kimi müəyyən edir, kibertəhlükəsizlik – kiberməkanda olan təhlükəsizlikdir. Standart kiberəthlükəsizliklik ilə şəbəkə təhlükəsizliyi, tətbiqi təhlükəsizlik, İnternet təhlükəsizliyi və kritik informasiya strukturlarının təhlükəsizliyi arasında əlaqəni qərb mütəxəssislərin nöqteyi-nəzərindən müəyyən edir. Beynəlxalq ekspertlətin fikrincə bütün bu terminləri "informasiya təhlükəsizliyi" anlayışı birləşdirir.

Beynəlxalq Telekommunikasiya İttifaqının X.1205 İTU-T tövsiyəsində "kibertəhlükəsizlik" kiberməkanın, təşkilatların və istifadəçilərin resurslarının müdafiəsi üçün istifadə oluna biləcək təhlükəsizliyin təmin edilməsi vasitələri, strategiyaları, prinsipləri, təhlükəsizliyin təmini tədbirləri, risqlərin idarə edilməsi üzrə rəhbər prinsiplər, yanaşmalar, hərəkətlər, peşəkar hazırlığı, praktiki təcrübə, sığorta və texnologiya kimi müəyyən edir.

Kiberməkan – informasiya-texniki infrastrukturu özündə ehtiva edən qlobal informasiya mühiti olub, bura məlumatların saxlanması, emalı, modifikasiyası və mübadiləsi üçün nəzərdə tutulan informasiya və telekommunikasiya şəbəkələri və kompüter sistemləri daxildir.

Kibertəhlükəsizlik fəlsəfi nöqteyi-nəzərdən müasir informasiya qarşıdurması şərtləri altında etibarlı və funksional davamlılığı saxlamaq sisteminin xüsusiyyəti və ya vəziyyətidir. Kibertəhlükəsizlik texniki mahiyyət baxımından müasir informasiya qarşıdurması şərtləri altında yüksək etibarlılıq və funksional davamlılığını təmin edən kompüter informasiya-idarəetmə sistemlərin informasiya təhlükəsizliyidir. Başqa sözlə desək, kibertəhlükəsizlik müasir informasiya qarşıdurması şərtləri altında kompüter informasiyası sahəsində informasiya təhlükəsizliyidir.

Məsələnin tarixi-müqayisəli aspektdə araşdırılması. Kibertəhlükəsizlik sahəsini araşdıran mütəxəssislərdən hesab edilən Fransisko Millarç İnternet-məkan və ona aid texnologiyalarla bağlı ideyaların aşağıdakı xronologiyasını təklif etmişdir: [4,12-15].

1. “Özün et” (DIY) və hər şeyi bilmək mədəniyyəti (1976-1984-cü illər). Həvəskarlar öz maşınlarını yaradır, proqram kodlarını işləyib hazırlayırdılar və kompüter klubları vasitəsilə fikir mübadiləsi aparırdılar. Bu, “Altair”, “Apple” və “Microsoft” kimi ilk şirkətlərin yarandığı dövrdür, lakin onların məhsulları bazarda çox cüzi yer tuturdu.

2. Real tətbiqlər və maşınlar (1984-1990-cı illər).

1984-cü ildə “AppleMac” tətbiqinin buraxılışı ilə qeyri-texnoloqlar informasiya texnologiyaları sahəsində üstünlük əldə edə bildilər. İstifadəçinin qrafik interfeysi (GUI), mətn prosessorları və elektron cədvəllər kimi tətbiqlər fərdi kompüterdən istifadə kimi bir irəliləyişə təkan verdi. Hətta istifadəsi çətin olan İBM kompüteri ofis ləvazimatları bazarında öz layiqli yerini tutdu.

3. “Hamımızı” əhatə edən pəncərələr (Windows) (1990-1993-cü illər).

1990-cı ildə “Microsoft Windows” ilk işçi variantı buraxıldı və böyük uğur qazandı. Hərçənd “Apple” şirkəti 1984-cü ildə “bizdən başqaları üçün kompüter” adlı şüarını yaratmışdı, “Microsoft” şirkəti əsas gəliri əldə edirdi. Bir sıra strateji səhvlər ucbatından “Apple” fərdi kompüter bazarında böyük hissəsini itirdi. “Microsoft” şirkəti “əhatə edək və genişləndirək” strategiyası ilə kompüter qiymətlərini inkişaf etmiş ölkələrdə orta sinfin ailələri üçün münasib səviyyəyə aşağı endirərək “bizdən başqalarını” özünə cəlb edə bildi. Bu, qızıl illər idi, belə ki, fərdi kompüterlər sənayesi istifadəçilərin böyük kütləsini yaratmışdı. Telekommunikasiyalar və media-industriya ilə konvergensiya ilə ittifaqda bu dövr texno-utopik idealların əsasını qoydu.

4) Şəbəkə utopiyası və kiberliberalizm (1993–1998-ci illər).

ABŞ hökuməti gözlənilmədən informasiya bazarına yeni postindustrial biznesində fəal iştirak edən akademik və hərbi ictimaiyyəti cəlb edir.

5) Texnorealizm (1998–?). Bu hərəkat Endryu Şapiro, Devid Şenk və Stiven Conson kimi intellektualların rəhbərliyi altında yaradılıb: [5,1-3]. Onlar səkkiz maddədən ibarət manifest nəşr etmişdilər.

1. Texnika neytral deyil. Ən böyük anlaşılmazlıq texnologiyaların qərəzdən tamamilə azad olması, onların qərarlarımıza və iş üsullarımıza təsir etməyən simasız artefaktlar olması fikridir. Əslində, texnologiyalar hər zaman müəyyən sosial, siyasi və iqtisadi ideyaların şüurlu və ya qəsdən əldə edilməsini nəzərdə tutur. Hər bir texniki qurğu ondan istifadə edən insanda dünyaya spesifik baxış və başqa insanlarla qarşılıqlı əlaqə üsullarını formalaşdırır. Texnologiyaların bu qərəzliliyini nəzərə almağımız və onun dəyərlərimizə və üstünlüklərimizə təsirini başa düşməyimiz çox vacibdir.

2. İnternet cəmiyyətdə inqilab hesab edilir, lakin bu, utopiya deyil. Şəbəkə - kommunikasiyalar sahəsində görkəmli ixtira olub, biznes, dövlət fəaliyyəti və şəxsi ünsiyyət üçün bir sıra yeni imkanlar açır. İnkişaf və artımdan asılı olaraq İnternet cəmiyyətin tam və dəqiq əksinə çevrilir. Maariflənmə və inkişaf vasitəsi olan İnternet eyni zamanda insan ruhunun bir sıra ziyanverici, təhrif edilmiş və ya bayağı hallarını da tirajlayır.

3. Dövlət elektron cəmiyyətdə çox mühüm rol oynamalıdır. Bəzi şəxslərin səylərinə baxmayaraq kiberməkan bütün planetdən ayrılmış xüsusi yursdiksiya zonası kimi nəzərdən keçirilə bilməz. Əlbəttə ki, dövlət kiberməkanda qəbul edilən adətlərə və qaydalara hörmət etməlidir və bu yeni mədəni dünyanı kobud müdaxiləsi və senzurası ilə boğmamalıdır, lakin cəmiyyətin şəbəkədə ayrı-ayrı vətəndaşların və korporasiyaların davranışlarına nəzarət etməmək hüququnun olmamasını düşünmək sadəcə axmaqlıqdır. Bütün vətəndaşlarının maraqlarının təmsilçisi, demokratik dəyərlərin təminatçısı rolunu reallaşdıran dövlət “virtual” cəmiyyətin inteqrasiyası barədə düşünməlidir.

4. İnformasiya hələ bilik deyil. Bizi əhatə edən dünyada informasiya çox sürətlə yayılır, daha ucuz və əlçatan olur. Bu cür uğurlar heyran etməyə bilməz. Lakin informasiyanın yayılması növbəti dəfə insan ağlına və skeptisizmə çağırışdır. Biz informasiyanın emalı və ya ötürülməsini onun daha çətin olan müdriklik və bilgilərə çevrilməsi ilə qarışdırmamalıyıq. Kompüterlərimiz nə qədər güclü olsalar da, onlar bizim idrak bacarıqlarımızı, qavrayış, düşünmə və qiymətləndirmə qabiliyyətlərimizi əvəz edə bilməzlər.

5. Bütün məktəblərin İnternetə qoşulması yaxşı haldır. Lakin məktəb təhsilinin problemləri olan kifayət qədər maliyyələşmənin olmaması, həddən artıq dolu siniflər, köhnəlmiş infrastruktur, standartların olmaması kimi məsələlərin texnologiya ilə heç bir əlaqəsi yoxdur. Pedaqoji ünsiyyət sənətini kompüterlər və ya İnternet ilə əvəzləmək mümkün deyil.

6. İnformasiya qorunmalıdır. Kiberməkan və başqa yeni texnologiyalar bizim müəllif hüquqlarımıza və intellektual mülkiyyətin müdafiəsi normalarına bir çağırışdır. İnternetdə olan informasiyanın digər KİV-də olduğu kimi qorunması üçün qanunları və onların təfsiri praktikasını yeniləmək lazımdır. Məqsəd eynilə qalmalıdır: müəlliflərə yeni əsərlər yaratmaq üçün kifayət qədər hüquqlar verilməldir, cəmiyyətə isə bu dəyərlərdən hamının xeyri üçün ədalətli şəkildə istifadə etmək hüququ verilməlidir.

7. Cəmiyyət elektron yayımda səsvermə hüququna malik olmalıdır. Bir sıra hallarda şəxsi provayder-korporasiyalar ictimai yayım vaxtını azaldır, informatika sahəsində ictimailəşdirmə sferasını məhdudlaşdırırlar. Vətəndaşların ictimai resurslardan, təhsil almaq, mədəni və sosial ehtiyaclarını ödəmək üçün televiziya və radio-kanallardan istifadə etmək imkanları olmalıdır. Biz ictimai mülkiyyətdə şəxsi istifadə hüququnu tələb etməliyik.

8. İnformasiya mədəniyyətinə malik olmaq vədəndaş davranışı sisteminin vacib komponenti olmalıdır. İnformasiya axınına məruz qalan dünyada aparat və proqramlar çox güclü sosial qüvvələrdir. Onların güclü tərəflərinin və çatışmazlıqlarının anlayışı, onların yaradılmasında və təkmilləşdirilməsinə iştirakı şəxsiyyətin vətəndaş hüquqlarının bir hissəsi kimi nəzərdən keçirilməlidir. Texniki qurğular əməl etməyə öyrəşdiyimiz qanunlar qədər həyatımıza təsir etməyə başlayıblar, ona görə də biz onlara demokratik nəzarətin müvafiq tədbirlərini tətbiq etməliyik.

Konnektivizm. Daha bir ideoloji istiqamət konnektivizm (ingilis sözü olan connect – birləşdirmək mənasını verir) adlanır. Kanadalı alim Devid T.Cons "konnektivizm" nəzəriyyəsində başlanğıc mövqe kimi bilgilər ilə şəbəkə arasında əlaqəni müəyyən etməyi təklif edir. Bunun üçün o, üç əsas bilgi növünü qeyd edir: [6, 12-10].

• keyfiyyət – yəni obyektlərin xassələri, əlaqələri və digər tipik görünən cəhətləri barədə bilgilər;

• kəmiyyət – yəni hissi qavrayış çərçivəsində cisimlərin tanınması və ya ayrılması üsulları ilə əldə edilən say, sahə, kütlə və digər əlamətlər haqqında biliklər;

• birləşdirən - yəni nümunələr, sistemlər, ekologiyalar və bu obyektlərin bir-biri ilə qarşılıqlı əlaqəsini anlamaqdan irəli gələn digər xüsusiyyətlər haqqında biliklər.

Bu üç biliklər növü arasında artan kontekst asılılıq effekti mövcuddur. Sensor informasiya, ilk növbədə, kontekstdən azaddır, lakin biz xassələri ayırmağa və adlandırmağa başlayanda, kontekst asılılıq artır. Obyektləri hesablamaq üçün onları fərqləndirməyə başlayanda onların kontekst asılılığı daha da artır. Birləşdirən bilgi - kontekstdə ən həssasdır, çünki o, yalnız qəbul edilən subyekt orijinal məlumatdakı nümunələri müəyyən etməyi öyrəndikdən sonra görünür.

"Şəbəkə biliyi" "ictimai bilik" və "şəxsi bilik" ilə eyni deyil. "Şəbəkə biliyi" anlayışı altında həm şəxsi, həm də ictimai biliyin əsasında dayanan xassələri və prosesləri nəzərdə tutur.

Cons qeyd edir ki, "bilik" adlandırdığımız hal obyektin hissələri arasında əlaqələrin və qarşılıqlı əlaqələrin nəticəsi olaraq (tərkib) obyektlərdə yaranır.

Buradan konnektivizmin iki növü yaranır. "Güclü konnektivizm" odur ki, "bilik" daxil edilmiş sistemin xüsusi fiziki quruluşu nəticəsində deyil, yalnız ümumi əlaqə yaratma mexanizmi nəticəsində yaranan əlaqələrdir. "Zəif konnektivizm", əksinə, obyektlərin fiziki xüsusiyyətlərinin əlaqələr yaratdığını və buna görə də biliklərin həmin obyektlər üçün fərdi olduğunu güman edir. Güclü və zəif konnektivizm birlikdə mövcud olmağa meyllidir [7, 23-30].

Kiberliberalizm və kiberrealizm. Bir qayda olaraq, kiberməkan üzrə Qərb mütəxəssisləri kiberliberalizm və kiberrealizm mövzusunu inkişaf etdirməkdə davam edirlər, lakin 2001-ci ildə baş vermiş dotkom qabarcığının partlayışına diqqət yetirməməyə çalışırlar. Bu iqtisadi qabarcıq 1995-ci ildən etibarən mövcud idi. Ənənəvi olaraq bu hadisə belə baş verib. Bu, internet-şirkətlərinin (əsasən Amerikanın) səhmlərinin qiymət artımı, böyük sayda yeni internet-şirkətlərinin yaranması və köhnə şirkətlərin XX əsrin sonunda internet bizneslə məşğul olması nəticəsində yarandı. Gəlir əldə etmək üçün İnternetdən istifadə etməyi təklif edən şirkətlərin səhmlərinin qiyməti sürətlə artdı. Bu cür yüksək qiymətlərə çoxsaylı şərhçilər və iqtisadçılar da haqq qazandırır və bildirirdilər ki, "yeni iqtisadiyyat" gəlib çatıb, əslində isə bu yeni bisnez-modellər qeyri-effektiv oldular, reklama xərclənən böyük vəsaitlər və böyük kreditlər iflas dalğasına, NASDAQ indeksinin güclü düşməsinə və server kompüterlərinin qiymətlərinin çökməsinə səbəb oldu [8, 20-33].

Lakin bunun arxasında azad ticarət və liberalizm ideyalarının dayanması bilərəkdən deyilmir. Qərb mütəxəssisləri kiberməkanın yeni münaqişə formaları, suverenlik formalarının dəyişilməsi, sıçrayış texnologiyaları və s. ilə əlaqəsi barədə danışmağa üstünlük verirlər, sanki yeni qabarcıq artıq heç vaxt təkrarlanmaya bilər. Lakin mobil qacetlərin və müxtəlif qurğuların yayılması bunun əksini deyir. Zəmanət hardadır ki, azad ticarətin əli inkişaf etmiş ölkələri yeni maliyyə-iqtisadi və siyasi dalana cəlb etməyəcək? Başqa sözlə desək, hərçənd kiberliberallar fəal şəkildə öz ideyalarını dəstəkləməkdə və ideologiyalarının üstünlüyünü sübut etməkdə davam etsələr də, əgər bu cür üsullar dövlət səviyyəsində qəbul edildiyi təqdirdə, onların strategiyalarının qeyri-münasib olması və nəinki milli, hətta beynəlxalq səviyyədə fəlakətə səbəb olacağı ilə bağlı aydın əlamətlər var.

Prinston Universitetinin sosiologiya və ictimai əlaqələr üzrə professoru "The American" Amerika liberal jurnalının həmredaktoru Pol Starr kiberməkanda kiberliberlizmin ideoloqlarından biri hesab edilir

[9,45-60]. Kiberliberalizm salnaməsinə daxil olan "Kiberhakimiyyət və azadlıq" adlı məqaləsində Pol Starr yazır ki, "kiberməkan siyasi ixtiranın və ictimai müqavilənin tək məhsuludur və yalnız qanun bizə ondan sərbəst istifadə etmək təhlükəsizliyini zəmanət verə bilər".

"Kiberməkan və Amerika arzusu: Bilik əsrinin Magna Cartası" (Cyberspace and the American Dream: A Magna Carta for the Knowledge Age) adlı məqalədə Corc Keyvort, Elvin Toffler və Ester Dayson yazırlar ki, " Üçüncü dalğa, Biliklər əsri başlayır, lakin mütərəqqi texnoloji və iqtisadi qüdrətinə sosial-siyasi hökmranlığı əlavə etmədən öz potensialını açmayacaq. Bu, İkinci Dalğa qanunlarının ləğvi və İkinci Dalğa münasibətlərinin təqaüdə göndərilməsi deməkdir. Bu, inkişaf etmiş demokratik ölkələrin liderlərinin üzərinə xüsusi məsuliyyət qoyur – asanlaşdırmaq, tələsmək və keçid dövrünü izah etmək. Bəşəriyyət yeni biliklərin "Elektron sərhədi"ni tədqiq edərkən o, ümumi rifah naminə özümüzü necə təşkil edəcəyimizlə bağlı ən dərin sualları yenidən gündəmə gətirməlidir.Azadlığın mənası, özünüidarəetmə strukturları, rəqabətin xarakteri, əməkdaşlıq şərtləri, mülkiyyətin tərifi, icma hissi və tərəqqinin xarakteri Biliklərin Əsrində 250 il bundan əvvəl yeni sənaye dövrü üçün yenidən baxıldığı kimi yenidən baxılacaqdır" [10,1-4].

Toffler, Keyvort və onların həmkarları kiberliberalizm haqqında əsərlərində öz əsl niyyətlərini ifadə edirlər: "...Bu yalnız yerində dayanan və keçmişin siqar baronlarına və bürokratlarına xidmət edən İkinci Dalğa qaydalarından, qanunlarından, vergilərindən azad olmaq deyil. Bundan sonra, əlbəttə ki, yaradılış - Amerika İdeyasının əbədi həqiqətlərinə əsaslanan yeni sivilizasiyanın yaradılması gəlməlidir".

Kiberməkanın yaranması ilə bağlı yeni istiqamətin ideoloqları öz ideyalarını liberal-sələfləri ilə əsaslandırırdılar. Çox vaxt libertarian düşüncəsinin müəlliflərindən sitatlar gətirilirdi, misal üçün, Ayn Rend, Elektron sərhəd anlayışı bizi Amerika ziyalılarının öz tarixi missiyasını ilahi hökmlə əsaslandırdıqları zamana - Manifest Destiny doktrinasının yaradılması dövrünə aparırlar.

Beləliklə, internet məkanı fərdi azadlığın, sahibkarlıq ruhunun və azad yaradıcılığın zəfər çalmalı olduğu, lakin bunun əsaslarının Amerikanın üstünlüyü sayəsində qoyulduğu yeni dünya adlandıran kiberlibertarizm meyli yarandı.

Nəticə

Məlumatların qloballaşması və iri texnologiya şirkətlərinin yaranması ilə məlumatların və məxfiliyin qorunması beynəlxalq münasibətlərdə mühüm məsələyə çevrilir. Məlumatların transsərhəd axını və məlumatların qorunması barədə müxtəlif qanunlar diplomatiya və beynəlxalq danışıqlar üçün çətin problemlər yaradır. Gələcəkdə beynəlxalq münasibətlərdə kibertəhlükəsizliyin gələcəyi fəal beynəlxalq əməkdaşlıq, qlobal kiberqayda və qanunların işlənib hazırlanması, həmçinin dövlət və qeyri-dövlət kiberfəaliyyətin idarə edilməsinə balanslaşdırılmış yanaşma ilə səciyyələndiriləcək. Bu, milli qüdrəti müəyyən edən, inkişaf etməkdə olan kiberməkanda naviqasiya üçün daimi adaptasiya və strateji planlanma tələb edən başlıca amil olacaq.

ƏDƏBİYYAT SİYAHISI:

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.s.3

2. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. -Washington D.C.: The White House, 2011.s.4

3. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.s.6

4. Francisco Millarch. Net ideologies: ideologies, in the outer and inner space.// Cybersociology Magazine, Issue 4. http://www.cybersociology.com/files/4_millarch. s.12-15

5. http://www.technorealism.org/ s.1-3

6. David T. Jones.A question (or two) on the similarity of "neuronal" and "networked" knowledge, The Weblog of (a) David Jones, March 5, 2011. s.12-20 http://davidtjones.wordpress.com/2011/03/05/a-question-or-two-on-the-similarity-of-neuronal-and-networked-knowledge/

7.George Siemens. Connectivism: A Learning Theory for the Digital Age. December 12, 2004.s.23-30

8. Paul Starr, The Creation of the Media: Political Origins of Modern Communications, Basic Books, 2004; Freedom's Power: The True Force of Liberalism, Basic Books, 2007. s.20-33

9. Paul Starr, Of Our Time: Cyberpower and Freedom MARCH 18, 2003.s.45-60 http://prospect.org/article/our-time-cyberpower-and-freedom

10. Esther Dyson, George Gilder, George Keyworth, and Alvin Toffler. Cyberspace and the American Dream: A Magna Carta for the Knowledge Age. Future Insight, Release 1.2, August 1994. s.1-4. http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html

XÜLASƏ

İnternet hər kəsin gündəlik həyatının bir hissəsinə çevrilib. O bizi artıq yalnız stasionar kompüterlər vasitəsilə deyil, həm də mobil qacetlər, Wi-Fi vasitəsilə ictimai yerlərdə çoxsaylı proqramlar və tətbiqlər vasitəsilə bir-birinə bağlayır. İnternetdən mal və xidmətlərin alqısı, maliyyə transaksiyaları, dövlət qurumlarına müraciət və başqa həyat üçün vacib ehtiyacların ödənilməsi üçün istifadə edilir. Kommunikasiya vasitəsi olmaqla yanaşı, İnternet həm xeyir, həm də şər məqsədlər üçün istifadə edilə bilən güclü siyasi silahdır. "Ərəb baharı" kimi tanınan Yaxın Şərqdəki etirazlar dalğası və dövlət çevrilişləri birbaşa bu texnologiyaların təsiri ilə bağlı idi və "Web 2.0" və ya "İnternet diplomatiyası" adını almışdır. Daha geniş kontekstdə bu prosesləri biz kibergeosiyasət adlandıra bilərik, belə ki, onlar münaqişə potensialına malik olaraq bütün dünyaya xasdır.

Təsadüfi deyil ki, Edvard Snoudenin açıqlamaları beynəlxalq münasibətlərin və təhlükəsizliyin kibertəhlükəsizlik sahəsində bazar şərtlərinə əhəmiyyətli dərəcədə təsir göstərdi və bir çox dövlətlərin dərhal reaksiyasına səbəb oldu. ABŞ rəsmi Pekini kiberşpionluqda günahlandıraraq "informasiya səs-küyü" yaratmağa çalışdı, Çin isə növbəsində rəsmi Vaşinqtona Ağ evin rəhbərliyi altında kəşfiyyat orqanında fəaliyyət göstərən və İnternetdən və mobil texnologiyalardan istifadə edən bütün vətəndaşlarını izləyən "Beş göz" barədə xatırlatdı.

İnternet siyasəti sahəsində aparılan ciddi dəyişikliklər fonunda dövlətlər iki düşərgəyə bölünüb: Qərb hesab edir ki, İnternet universal olmalıdır (lakin İnterneti kəşf edən ABŞ-nin nəzarəti altında olmalıdır), bu düşərgəyə müqavimət göstərən dövlətlər isə internet məkan da daxil olmaqla, öz suverenliyini qorumağa çalışırlar. Hərçənd bu qarşıdurma qlobal siyasi gündəliklə bağlı olsa da, bir sıra dövlətlərin daxilində son illər birbaşa kiberməkanla bağlı olan qanunvericilik səviyyəsində ciddi debatlar və dəyişikliklər aparılmışdır. Ənənəvi politologiya və klassik geosiyasət üçün bu proseslər mürəkkəb və çox vaxt aydın olmayan fenomendir. Problem ondan ibarətdir ki, kiberməkanla bağlı məsələlərin bir hissəsi yüksəkixtisaslı mütəxəssislərin sahəsidir, belə ki hüquqşünaslar mühəndis və proqramçıların köməyi olmadan təfərrüatlardan baş çıxarda bilməyəcəklər, siyasətçilər isə yalnız yeni imkanlarla bağlı istehlakçıların maraqları ilə yanaşı, kiberməkanın texniki və siyasi aspektlərini də başa düşməlidirlər. Ona görə də yalnız siyasi və iqtisadi aspektlərə diqqət yetirmək deyil, həmçinin ideoloji, sosial və hərbi səviyyələri, yəni hər bir dövlətin və ya alyansın geosiyasi strukturunun elementlərini analiz etmək lazımdır.

Kiberməkan azadlıq, ticarət və iqtisadi artım sahəsi olaraq qalmalıdır. Müasir cəmiyyətin çiçəklənməsinin və tərəqqisinin şərti olan kibertəhlükəsizlik indi beynəlxalq münasibətləri tənzimləyən hakimiyyətlərin strategiyalarının elementi və qüvvələr nisbətinə çevrilmişdir.

Açar sözlər: *kibertəhlükəsizlik, kibercinayətkarlıq, kiberməkan, informasiya-kommunikasiya texnologiyaları (İKT).*

SUMMARY

The problem of cyber security in international relations

The Internet has become a part of everyone's daily life. It connects us not only through desktop computers, but also through mobile gadgets, Wi-Fi in public places through numerous programs and applications. The Internet is used to purchase goods and services, make financial transactions, apply to government agencies, and satisfy other vital needs. In addition to being a means of communication, the Internet is a powerful political weapon that can be used for both good and evil purposes. The wave of protests and coups d'état in the Middle East, known as the "Arab Spring", was directly related to the influence of these technologies and received the name "Web 2.0" or "Internet diplomacy". In a broader context, we can call these processes cybergeopolitics, as they are global in their potential for conflict.

It is no coincidence that the revelations of Edward Snowden significantly affected the market conditions in the field of cyber security of international relations and security and caused an immediate reaction of many states. The US official tried to create "information noise" by accusing Beijing of cyber-espionage, while China, in turn, reminded Washington of the "Five Eyes", an intelligence agency under the leadership of the White House that monitors all its citizens using the Internet and mobile technologies.

Against the background of serious changes in the field of Internet policy, the states are divided into two camps: the West believes that the Internet should be universal (but it should be under the control of the United States, which discovered the Internet), and the states that resist this camp try to protect their sovereignty, including the Internet space. Although this conflict is related to the global political agenda, serious debates and changes have been made at the level of legislation directly related to cyberspace within a number of states in recent years. For traditional poli-

tical science and classical geopolitics, these processes are complex and often unclear phenomena. The problem is that some issues related to cyberspace are the domain of highly qualified specialists, as lawyers cannot understand the details without the help of engineers and programmers, while policymakers must understand the technical and political aspects of cyberspace in addition to the consumer interests of new opportunities. Therefore, it is necessary to pay attention not only to the political and economic aspects, but also to analyze the ideological, social and military levels, that is, the elements of the geopolitical structure of each state or alliance.

Cyberspace must remain an area of freedom, commerce and economic growth. Cyber security, which is a condition for the prosperity and progress of modern society, has now become an element of the strategies of the authorities regulating international relations and the balance of powers.

Keywords: *cyber security, cybercrime, cyberspace, information and communication technologies (ICT).*

РЕЗЮМЕ

Проблема кибербезопасности в международных отношениях

Интернет стал частью повседневной жизни каждого человека. Он связывает нас не только через настольные компьютеры, но и через мобильные гаджеты, Wi-Fi в общественных местах, через многочисленные программы и приложения. Интернет используется для приобретения товаров и услуг, совершения финансовых операций, обращения в государственные органы и удовлетворения других жизненно важных потребностей. Помимо того, что Интернет является средством общения, он является мощным политическим оружием, которое можно использовать как во благо, так и во зле. Волна протестов и государственных переворотов на Ближнем Востоке, известная как «арабская весна», была напрямую связана с влиянием этих технологий и получила название «Веб 2.0» или «интернет-дипломатия». В более широком контексте мы можем назвать эти процессы кибергеополитикой, поскольку они глобальны по своему конфликтному потенциалу.

Не случайно разоблачения Эдварда Сноудена существенно повлияли на конъюнктуру рынка в сфере кибербезопасности международных отношений и безопасности и вызвали немедленную реакцию многих государств. Американский чиновник попытался создать «информационный шум», обвинив Пекин в кибершпионаже, а Китай, в свою очередь, напомнил официальному Вашингтону о «Пяти глазах» — спецслужбе под руководством Белого дома, которая следит за всеми своими гражданами с помощью Интернет и мобильные технологии.

На фоне серьезных изменений в сфере интернет-политики государства разделились на два лагеря: Запад считает, что Интернет должен быть универсальным (но он должен находиться под контролем США, открывших Интернет), и государства, противостоящие этому лагерю, пытаются защитить свой суверенитет, в том числе в интернет-пространстве. Хотя этот конфликт связан с глобальной политической повесткой дня, в ряде государств за последние годы произошли серьезные дискуссии и изменения на уровне законодательства, непосредственно связанного с киберпространством. Для традиционной политической науки и классической геополитики эти процессы представляют собой сложные и зачастую неясные явления. Проблема в том, что некоторые вопросы, связанные с киберпространством, являются прерогативой высококвалифицированных специалистов, поскольку юристы не могут разобраться в деталях без помощи инженеров и программистов, в то время как политики должны понимать технические и политические аспекты киберпространства в дополнение к потребительским интересам новых возможности. Поэтому необходимо уделять внимание не только политическим и экономическим аспектам, но и анализировать идеологический, социальный и военный уровни, то есть элементы геополитической структуры каждого государства или альянса.

Киберпространство должно оставаться зоной свободы, торговли и экономического роста. Кибербезопасность, являющаяся условием процветания и прогресса современного общества, сегодня стала элементом стратегий властей, регулирующих международные отношения и баланс сил.

Ключевые слова: *кибербезопасность, киберпреступность, киберпространство, информационно-коммуникационные технологии (ИКТ).*