AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
AZƏRBAYCAN DİLLƏR UNİVERSİTETİ

Əlyazması hüququnda

LÜTFİYYƏ ZAVUR qızı ƏLİZADƏ

MÜASİR DÖVRDƏ ABŞ-ın İNFORMASİYA MÜHARİBƏSİ

İxtisaslaşma: HSM – 060211 - Regionşünaslıq (Amerikaşünas)
Magistr elmi dərəcəsi almaq üçün
təqdim olunmuş

DİSSERTASİYA

Elmi rəhbər: _____
K.C.Ağayeva
fəlsəfə üzrə fəlsəfə doktoru, dosent

Bakı-2017

MÜNDƏRİCAT

GİRİŞ

Mövzunun aktuallığı. Müasir dövrdə informasiya müharibələri və bu müharibələrdə ABŞ-ın iştirakı elmi cəhətdən öyrənilməsi tələb olunan məsələlərdəndir.

Qloballaşma şəraitində beynəlxalq arenada baş verən proseslər dövlətləri öz informasiya məkanına nəzarəti gücləndirməyə vadar edir. Dövlətlər informasiya infrastrukturlarına ziyan vura biləcək təbii və süni xarakterli, təsadüfi və ya qəsdən törədilmiş təsirlərin qarşısını almağa, özlərinin informasiya təhlükəsizliyini təmin etməyə çalışırlar. İstənilən dövlətin informasiya məkanına dəyən zərbə yalnız onun informasiya infrastrukturuna deyil, eyni zamanda siyasi, iqtisadi, hərbi, mədəni infrastrukturuna da böyük ziyan vurur. İnformasiya texnologiyalarının inkişafında kifayət qədər uğur qazanan ABŞ, həm də informasiya təhdidləri ilə ən çox üzləşən ölkədir. Bütün bunlar ona səbəb olmuşdur ki, hələ keçən əsrin 90-cı illərinin birinci yarısından başlayaraq ABŞ milli informasiya sistemlərinin və informasiya infrastrukturunun təhlükəsizliyinin təmin olunması üçün tədbirlər görür. ABŞ-ın informasiya təhlükəsizliyi sahəsində atdığı addımlar, onların mənfi və müsbət cəhətləri elmi tədqiqat obyekti kimi maraq doğurur, bu da dissertasiya mövzusunun aktuallığına dəlalət edir.

2001-ci il 11 Sentyabr hücumları ABŞ-ın kəşfiyyat strukturlarının təkmilləşdirilməsində ciddi rol oynamışdır. Bu hadisələr kəşfiyyat strukturlarında islahatların həyata keçirilməsinin vacib olduğunu bir daha göstərdi. Bununla əlaqədar olaraq, informasiya və təhlükəsizliklə bağlı olan strukturlar yenidən təşkil olundu. Bu zaman milli informasiya təhlükəsizliyinin təmin edilməsi məsələləri ön plana çıxarıldı. Bu tədbirlərin həyata keçirilməsi zamanı əldə olunan təcrübə istənilən ölkənin informasiya təhlükəsizliyini təmin etmək işində nəzərə alına bilər. Bu məqam da öyrənilən mövzunun əhəmiyyətini göstərir.

Sosial həyatda xüsusi yeri olan medianın fərd, cəmiyyət, mədəniyyət və nəhayət, siyasi sahə ilə olan əlaqəsi danılmazdır. Məlumdur ki, informasiya müharibələrində medianın rolu böyükdür. ABŞ media korporasiyaları müasir dövrdə

baş verən informasiya müharibələrində öz əhəmiyyətinə, əhatə dairəsinə, təsir imkanlarına görə bir çox ölkələrin media korporasiyalarından fərqlənir. Amerika Birləşmiş Ştatları bu gün informasiya texnologiyalarını istehsal edən, inkişaf etdirən və ixrac edən əsas ölkədir. Media texnologiyaları və informasiya sahəsindəki tərəqqi ABŞ-ın rabitə sisteminə və xəbər siyasətinə də əhəmiyyətli şəkildə təsir etmiş, onların fəaliyyət dairəsini xeyli genişləndirmişdir. ABŞ media koorporasiyalarının qlobal təsirə malik olması və onların fəaliyyəti ilə bağlı məqamların elmi cəhətdən təhlil olunması da öyrənilən mövzunun aktual olduğunu sübut edir.

İnformasiya təhlükəsizliyinin təmin olunması, təcavüzkar Ermənistanın və onun havadarlarının işğalçılıq siyasəti ilə üz-üzə qalan Azərbaycan Respublikası üçün də aktualdır. Bu sahədə respublikada ciddi addımlar atılmış, müasir tələblərə cavab verən informasiya şəbəkələri yaradılmışdır. Eyni zamanda Azərbaycan qlobal informasiya məkanının fəal aktorlarından biridir, informasiya təhlükəsizliyi sahəsində beynəlxalq birliklərlə, o cümlədən ABŞ-la əməkdaşlıq edir. Müraciət olunan mövzunun araşdırılması, bu zaman əldə olunan nəticələr qeyd olunan əməkdaşlığın daha da genişləndirilməsinə öz töhfəsini verə bilər.

Mövzunun öyrənilmə dərəcəsi. Tədqiqat prosesində mövzu ilə bağlı mövcud ədəbiyyat bazasından, nəşr olunmuş rəsmi sənədlərdən geniş istifadə olunmuşdur. Dissertasiya işinin yazılmasında azərbaycan türk,rus vəingilis dillərində olan ədəbiyyatlardan, jurnallardan, internet resurslarından istifadə edilmişdir. İnformasiya müharibəsinin mahiyyəti, həyata keçirilmə üsulları və formalarına həsr olunmuş əsərlər də tədqiqat zamanı daim diqqət mərkəzində olmuşdur. Bu əsərlərə misal olaraq D. Stupples, D. T. Kuehl, D. Denning, J. Arquilla, A. Vəliyeva, E. Talışınski və başqalarının tədqiqatlarını göstərmək olar. Magistrlik dissertasiyasının yazılması zamanı M. Libikinin “İnformasiya müharibəsi nədir?”, T. Ronanın “Silah sistemləri və İnformasiya Müharibəsi”, R. Molanderin “Strateji informasiya müharibəsi: Müharibənin yeni üzü”, M. Sağsanın “İnformasiya müharibəsi: Sipərlərdən klavyaturalara daşınan hərəkatın anatomiyası”, İ. Ələkbərovanın “İnformasiya Müharibəsi Texnologiyalarının analizi və təsnifatı” əsərlərindən istifadə olunmuşdur. Qeyd olunan əsərlərdə informasiya müharibəsinin yaranması və sürətli inkişafı,

müasir informasiya müharibəsi texnologiyalarının növləri, onun həyata keçirilmə vasitələri, informasiya müharibəsinin yeni yaranmış formalarından biri olan strateji informasiya müharibəsinin mahiyyəti təhlil edilmişdir.

ABŞ-ın silahlı qüvvələrində şəbəkə strukturana həsr olunmuş əsərlər sırasında C. Greyin "Başqa bir Qanlı Əsr: Gələcək Müharibə", A.Bedritskiyin "İnformasiya müharibəsinin müasir konsepsiyası", A. Mevlutoğlunun "Şəbəkə mərkəzli müharibə üzərinə qeydlər", D. S. Albertsin "Şəbəkə mərkəzli müharibə: İnformasiya üstünlüyünün təmin edilməsi və ondan istifadə edilməsi" əsərlərini qeyd etmək olar. Adı çəkilən əsərlərdə şəbəkə müharibəsi termininin izahı, ABŞ silahlı qüvvələrində istifadə olunan informasiya texnologiyalarıdan bəhs olunmuşdur. Bu əsərlərdə yer almış faktik materiallardan da iş prosesində istifadə olunmuşdur.

Tədqiqat prosesinə cəlb edilmiş və informasiya müharibələrində ABŞ-ın media korparasiyalarının fəaliyyətinə həsr olunmuş əsərlərə misal olaraq S. Livinqstonun "CNN effektini aydınlaşdırmaq", N. Çomskinin "Əsas axın mediasını vacib edən nədir?", E. İlhan və N. Dirikin "Müharibə xəbərləri kontekstində xəbər siyasətləri: ABŞ nümunəsi", M. H. Belknepin "CNN effekti: Strateji dəstək və ya əməliyyat riski?" və s. göstərmək olar.

N. Kşetrinin "Kibertəhlükəsizlik və Beynəlxalq Münasibətlər: ABŞ-ın Çin və Rusiya ilə Nişanı", F. Sezginin "Eduard Snouden hadisəsinin ABŞ-Rusiya münasibətlərinə təsiri", R. Nurəddinoğlunun "ABŞ-ın Avropanı gizli dinləməsi" əsərləri ABŞ-ın Rusiya və Çin ilə apardığı informasiya müharibəsi, Avropa ilə ABŞ arasında yaşanan gərginliklər və bütün bunların onun xarici siyasətinə göstərdiyi təsirin əhəmiyyətindən, ölkələrlərarası münasibətlərdə informasiya sahəsində mövcud olan rəqabətə həsr edilmişdir.

İstifadə olunmuş materiallar arasında dövri mətbuat və İnternet resursları da əhəmiyyətli yer tutur.

Qeyd olunan materiallardan istifadə bir tərəfdən problemin hansı səviyyədə öyrənildiyini aşkara çıxarmağa, digər tərəfdən tədqiqatı tarixi və mövcud siyasi reallıqlar nəzər alınmaqla sistemli şəkildə aparmağa kömək etmişdir.

Tədqiqatın obyekti. Tədqiqatın obyektini müasir dövrdə ABŞ-ın informasiya siyasəti və həyata keçirdiyi informasiya müharibələri təşkil edir.

Tədqiqatın predmeti. Müasir dövrdə informasiya müharibəsinin xarakterik xüsusiyyətləri, ABŞ-ın informasiya təhlükəsizliyinin federal qanunvericiliklə tənzimlənməsi, "CNN", "The New York Times", "Associated Press" kimi qlobal media korporasiyalarının informasiya müharibələrində iştirakı, informasiya müharibələrinin tərkib hissəsi olan şəbəkə müharibələri və ABŞ silahlı qüvvələrində şəbəkə strukturu, Rusiya, Çin kimi böyük dövlətlərlə aparılan informasiya müharibələrinin ABŞ-ın xarici siyasətinə təsiri tədqiqat işinin predmetinə daxildir.

Dissertasiyanın məqsəd və vəzifələri.Tədqiqat işinin əsas məqsədi müasir dövrdə ABŞ-ın informasiya müharibəsi, bu müharibənin həyata keçirilmə formaları və onun regional və beynəlxalq münasibətlərə təsirini öyrənməkdən ibarətdir.

Müəyyən olunmuş məqsədə çatmaq üçün aşağıdakı vəzifələri yerinə yetirmək nəzərdə tutulur:

- informasiya müharibəsinin xarakterik xüsusiyyətlərini təhlil etmək;
- federal qanunvericiliyin informasiya təhlükəsizliyinin təmin olunması istiqamətindəki rolunu müəyyənləşdirmək;
- müasir dövrdə aparılan informasiya müharibələrində ABŞ-ın media korporasiyalarının iştirakını araşdırmaq;
- ABŞ-ın informasiya müharibəsində onun silahlı qüvvələrinin şəbəkə strukturunun roluna aydınlıq gətirmək;
- müasir dövrdə ABŞ-ın informasiya müharibəsinin onun xarici siyasətinə təsirini təhlil etmək.

Tədqiqatın metodoloji əsasları: Magistr dissertasiyasının yerinə yetirilməsi zamanı müxtəlif metodlardan istifadə olunmuşdur. İş prosesində qarşıya qoyulan məqsədlərə çatmaq, müasir dövrdə ABŞ-ın informasiya müharibəsinin xarakterik xüsusiyyətlərini təhlil etmək, problemlərin mahiyyətini açmaq, ümumiləşdirmələr aparmaq prosesində müqayisəli təhlil, sintez, deduksiya və induksiya kimi metodlar tətbiq olunmuşdur.

Dissertasiyanın elmi yeniliyi. Məlum olduğu kimi, ABŞ-ın Rusiya və Çin kimi böyük dövlətlərlə informasiya müharibəsinə dair müxtəlif səpkili əsərlər yazılmışdır. Problem ətrafında ədəbiyyat bazası mövcud olsa da, ABŞ-ın informasiya müharibəsinin əhatəli təhlili ilə bağlı ilkin mənbələr Azərbaycanda elmi dövriyyəyə məhz bu işlə gətirilmişdir. Bundan əlavə, ABŞ-ın media korporasiyalarının informasiya müharibələrində iştirakı, silahlı qüvvələrdə şəbəkə strukturu və şəbəkə müharibələrinin ətraflı formada tədqiq edilməsi, eyni zamanda mövzunun azərbaycanlı müəllif tərəfindən neytral şəkildə qiymətləndirilməsini də tədqiqatın elmi yenilikləri sırasına daxil etmək olar.

Tədqiqat işinin təcrübi əhəmiyyəti. Dissertasiyanın özündə ehtiva etdiyi məlumatlar, alınan nəticələr və aparılmış ümumiləşdirmələr ABŞ-ın müasir dövrdə informasiya müharibələrində iştirakı ilə bağlı bir çox suallara aydınlıq gətirilməsi baxımından əhəmiyyətlidir.

İş prosesində əldə olunmuş nəticələr öyrənilən problemlə bağlı müəyyən proqnozların verilməsinə və qiymətləndirmələrin aparılmasına yardım edə bilər. Bundan başqa, dissertasiyanın materialları əsasında ABŞ-ın rəqibləri ilə apardığı informasiya müharibəsi, Ağ Evin xarici siyasətində informasiya təhlükəsizliyinin rolu və əhəmiyyəti ilə bağlı tədqiqatların aparılması, analitik materialların hazırlanması mümkündür.

Tədqiqat işində yer almış materiallar problemlə bağlı dərsliklərin, metodik vəsaitlərin, tədris proqramlarının, mühazirə mətnlərinin hazırlanmasında da əhəmiyyətli ola bilər.

Tədqiqat işinin aprobasiyası. Magistrlik dissertasiyasının əsas müddəaları, müəllifin dərc olunmuş, aşağıda göstərilmiş məqalə və tezislərində öz əksini tapmışdır:

1. Əlizadə L. ABŞ-ın informasiya əməliyyatları // Ümummilli Lider Heydər Əliyevin anadan olmasının 93-ci ildönümünə həsr olunmuş illik konfransdakı məruzələrin tezisləri (II Hissə). Bakı 2016. s. 297-298.

2. Əlizadə L. ABŞ-ın rəqəmsal kəşfiyyat sistemləri və dünyadaki tətbiqi // XIV Beynəlxalq tələbə elmi-praktik konfransının materialları. Qərb Universiteti, Bakı 2016. s. 270-271.
3. Əlizadə L. ABŞ silahlı qüvvələrində şəbəkə strukturu // (ADU-nun Elmi Xəbərləri, №3 - çapdadır).
4. Əlizadə L. ABŞ-ın informasiya təhlükəsizliyinin təmin olunması sahəsində federal qanunvericilik // (Beynəlxalq münasibətlərin aktual problemləri, №1 - çapdadır).

Dissertasiyanın strukturu. Magistr dissertasiyası "Giriş", iki fəsil, altı paraqraf, "Nəticə" və "İstifadə olunmuş ədəbiyyat siyahısı"ndan ibarətdir.

FƏSİL 1. MÜASİR DÖVRDƏ ABŞ-ın İNFORMASİYA SİYASƏTİNİN ƏSASLARI

1.1. İnformasiya müharibəsinin mahiyyəti və xarakteri

Müasir dövrdə beynəlxalq arenada baş verən proseslər dövlətləri öz informasiya məkanına nəzarətigücləndirməyə vadar edir. Dövlətlərinformasiya infrastrukturlarına ziyan vura biləcək təbii və süni xarakterli, təsadüfi və ya qəsdən törədilmiş təsirlərin öhdəsindən gəlməklə özlərinin informasiya təhlükəsizliklərini təmin etməyə çalışırlar. İstənilən dövlətin informasiya məkanına dəyən zərbə yalnız onun informasiya infrastrukturuna deyil, eyni zamanda siyasi, iqtisadi, hərbi, mədəni infrastrukturuna da böyük ziyan vurur.

Beynəlxalq arenada həm ölkələrin daxilində, həm də qlobal miqyasda informasiya axınının sərbəst olması, biznes, beynəlxalq əlaqələr və sosial inteqrasiya üçün olduqca vacibdir.Hətta informasiya müəyyən bir hərbi qüvvənin döyüş qabiliyyəti üçün də olduqca çox əhəmiyyətlidir. Kommunikasiya bu gün, sıx şəkildə internet vasitəsilə, yerüstü rabitə şəbəkələri və ya kosmosdakı peyk şəbəkəsi vasitəsilə həyata keçirilir [72].

Əks tərəfin informasiya resurslarını ələ keçirən dövlət üçün bu resurslar və onlardan əldə edilən bilik, öz gücünü artırmaq, bütün sahələrdə rəqibdən üstün olmaq və gələcəkdə onun istənilən sahədə hücumlarını dəf etmək, eyni zamanda, öz maddi-mənəvi dəyərlərini qorumaq üçün bir vasitədir. Odur ki, dövlətin informasiya resursu çox zaman strateji resurs hesab edilir və analoji olaraq vacib xammal ehtiyatı, enerji, faydalı qazıntılar və s. resursları ilə eyni səviyyədə qiymətləndirilir. İnformasiya axınları üçün sərhədlərin şəffaflığı dövlət hakimiyyət orqanlarının funksiyalarında prinsipial olaraq başqa bir situasiya yaratmış, informasiya sistemlərinin dövlətlərin infrastrukturuna (bankmaliyyə, nəqliyyat, elektrik şəbəkələri, neft və qaz xətləri) tətbiq edilməsi isə onları informasiya müharibəsində potensial obyektlərə çevirmişdir.

İnformasiya müharibəsi nədir? Bu suala cavab vermək üçün ilk növbədə-müharibə nədir?-sualına cavab tapmaq lazımdır. Hərbi və milli təhlükəsizlik konsepsiyasının tərəfdarları Karl fon Klauzevitsin "müharibə bir hərəkatdır, şiddət atmosferidir" fikri ilə razılaşırlar[49, 27].

Güc və şiddətin səbəbi istənilən siyasi aktorun öz varlığını, iradəsini başqa birinə qəbul etdirməsidir. İnformasiya müharibəsində isə siyasi aktorlar bu gücü informasiya vasitəsilə həyata keçirirlər[49, 47].

İnformasiyanın müharibələrdə silah kimi istifadə edilməsi yeni fikir deyil. İnformasiya müharibəsinin (İM) tərifini başa düşmək üçün ən bariz nümunələrdən biri orduda informasiyadan necə istifadə olunmasına diqqət yetirilməsidir [75, 2]. Müharibə, döyüş əməliyyatları aparmadan İM həyata keçirmək mümkündür, lakin İM olmadan fiziki müharibə aparılmır. Başqa sözlə, müharibə aparılarkən, döyüşlərə başlayarkən onun tərkib hissəsi kimi İM-in həyata keçirilməsi zəruri şərtlərdən biri hesab olunur. Məsələn, Çingiz xanın apardığı müharibələr zamanı ordudan əvvəl düşmənin sıralarına, yaşayış məskənlərinə xüsusi informasiya hazırlığı görmüş atlılar (xəbərçilər, carçılar) göndərilirdi. Onların əsas vəzifəsi Çingiz xanın ordusunun hədsiz dərəcədə güclü və amansız əsgərlərdən təşkil olunduğu haqqında xəbərlər yayaraq əhalidə qorxu, ruh düşkünlüyü yaratmaq idi. Bu cür psixoloji təsir üsullarından digər məşhur sərkərdələr (Makedoniyalı İsgəndər, Teymurləng və s.) də istifadə etmişdir. İkinci dünya müharibəsi zamanı Hitler və Stalin də informasiya-psixoloji təsirin əhəmiyyətini yaxşı dərk edirdilər və bu üsuldan istifadə edirdilər[31, 81].

İlk dəfə "informasiya müharibəsi" termini 1976-cı ildə amerikalı mütəxəssis Tomas Rona (Thomas Rona) tərəfindən "Boeing" şirkəti üçün hazırladığı "Silah sistemləri və informasiya müharibəsi" adlı hesabatında istifadə edilmişdir. T.Rona hesabatında qeyd edir ki, son illərdə informasiya infrastrukturu ABŞ iqtisadiyyatının əsas komponentlərindən birinə çevrilmişdir[64, 5].

"İnformasiya müharibəsi" termini rəsmi olaraq isə ilk dəfə ABŞ Müdafiə Nazirliyinin 1992-ci il 21 dekabr tarixli, 3600.1 saylı direktivində öz əksini tapmışdır [29, 82].

ABŞ-ın Milli Müdafiə Universitetinin əməkdaşı Martin Libiki "informasiya müharibəsi" anlayışına belə tərif vermişdir: "İnformasiya müharibəsini başa düşmək, kor insanların fili tanımaq səyinə bənzəyir. Filin ayağına toxunan şəxs onu ağaca, quyruğuna toxunan isə kəndirə bənzədir. İnformasiya müharibəsinin əlamətləri də buna bənzər şəkildə qəbul edilir. Bəs bu üsulla tam təsəvvür almaq mümkündür? Bəlkə də fil yoxdur, fil olmağa cəhd edən ağac və kəndir var. Mütəxəssislərin bir qrupu bu anlayış altında bir çox istiqamətləri birləşdirmək istədikləri halda, digərləri informasiya müharibəsinin hərhansı aspektini ümumi anlayış kimi qəbul edir..." [51, 3]. M.Libikinin bu fikri "informasiya müharibəsi"nin çox geniş anlayış olmasıilə bağlı mövcud olan fikirləri təsdiqləyir.

ABŞ-ın Müdafiə Nazirliyinin sənədlərində qeyd olunur ki, İM-də informasiya həm silah, həm də məqsəddir. İnformasiya hücumu isə icazə alınmadan istənilən formada informasiyanın köçürülməsinə, dəyişdirilməsinə, məhvinə, eyni zamanda proqram təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatdır [39].

ABŞ-da İM-i təsvir etmək üçün çox vaxt onu informasiya əməliyyatı ilə müqayisə edirlər. İnformasiya əməliyyatı-məqsədə çatmaq üçün qarşı tərəfin informasiya fəzasına təsir etmək və bu zaman öz informasiya resurslarını qorumaq məqsədi ilə xüsusi metodlardan və vasitələrdən (siyasi, iqtisadi, texniki, hərbi və s.) istifadə etməklə reallaşdırılan mübarizə formasıdır [38].

Rusiyalı mütəxəssislər bu mübarizə formasını informasiya qarşıdurması kimi təsvir edirlər. İnformasiya qarşıdurması-tərəflərin elə mübarizə formasıdır ki, bu zaman onlar xüsusi metodlardan, informasiya resurslarına təsir üsullarından və vasitələrindən istifadə etməklə qarşı tərəfin informasiya resurslarına birbaşa təsir göstərmək imkanına malik olurlar[28, 127-130].

Amerika tədqiqatçılarının fikrincə, informasiya əməliyyatı vasitələrilə realizə olunan informasiya qarşıdurması hərbi qüvvələrin, elmi mərkəzlərin, müxtəlif siyasi təşkilatların hazırlığında və fəaliyyətində İM texnologiyalarından geniş formada istifadəni nəzərdə tutur [58].

İnformasiya qarşıdurmasında əsas məqsəd qarşı tərəfin informasiya da daxil olmaqla, bütün növ resurslarına təsir göstərə bilməkdir. İnformasiya qarşıdurmasının effektivliyinin əsas meyarı kimi qarşı tərəfə məxsus olan şəbəkə və kommunikasiya texnologiyalarına, nəhayət, kompyuterlərə icazəsiz müdaxilələr nəzərdə tutulur. Digər tərəfdən, informasiya qarşıdurmasında demoqrafiya, təbliğat, "beyinlərin yuyulması", ictimai rəyin və şüurun manipulyasiyası və s. kimi üsullardan geniş şəkildə istifadə olunur. İM prosesində kompyuter şəbəkəsinə daxil olmaqla, qarşı tərəfin mühüm əhəmiyyət kəsb edən maliyyə, bank sistemi, rabitə, elektrik təchizatı və nəqliyyat vasitələrini iflic etmək mümkündür. Bu məqsədlə İnternetdə veb-briqadalar və xakerlər fasiləsiz fəaliyyət göstərirlər. Onlar xüsusi təşkil edilmiş və fəaliyyətləri müəyyən hədəflərə yönəldilmiş peşəkarlardan ibarətdir. İM-dəinformasiyakommunikasiya sistemlərinin normal iş fəaliyyətinin pozulması, psixoloji-ideoloji informasiyası, informasiya blokadası və s. informasiya əməliyyatlarından geniş şəkildə istifadə edilir[1, 82].

İM zamanı maraq obyektləri informasiya sistemləri və informasiya mübadiləsi şəbəkələri olur. Bu şəbəkələrə informasiya sistemi mərkəzi, xüsusi informasiya emal edən ötürülmə xətləri, İM-də iştirak edən İKT vasitələri aid edilir. İnformasiya müharibəsi mərhələlərlə aparılmalı və bu zaman məqsəd və hədəflər dəqiq müəyyən edilməlidir. İnformasiya müharibəsinin mərhələləri bunlardır:

1. Məqsədin müəyyən edilməsi. "İnformasiya müharibəsi nə üçün lazımdır?" və "nəticədə nə əldə ediləcəyi gözlənilir?" suallarına cavab tapılması;
2. Strategiyanın müəyyən edilməsi. Burada İKT-nin dörd baza komponenti nəzərə alınmalıdır:

- informasiyanın hazırlanması;
- informasiyanın yönələcəyi kommunikasiya kanalının təyin edilməsi;
- informasiyanın təsiri altına düşəcək auditoriyanın müəyyənləşdirilməsi;
- informasiya müharibəsi texnologiyasının seçilməsi;

3. Taktiki fəaliyyət planının hazırlanması.

"İnformasiya müharibəsi" anlayışı terminoloji cəhətdən hazırda daha çox elektron kütləvi informasiya vasitələrinin, informasiya və telekommunikasiya

texnologiyalarının, informasiya resurslarının sürətli inkişafının nəticəsi olaraq daha da geniş istifadə olunmağa başlanmışdır[6].

Tofflerlər "Müharibə və müharibəyə qarşı" məqaləsində yazırlar ki, informasiya texnologiyaları sadə cəmiyyətləri informasiyaya əsaslanan cəmiyyətlərə çevirirlər [83, 7].

Ən dar mənada informasiya müharibəsi "münaqişələrin reallaşması üçün informasiyadan istifadə edilməsi" kimi təsəvvür olunur [34]. Ən geniş mənada informasiya müharibəsi isə "insan əlaqələrinin və qarşıdurmaların ortaya çıxması ilə başlayan mübarizə forması" kimi qeyd olunur [50].

"İnformasiya müharibə"si problemi bir çox ölkədə araşdırılmışdır. ABŞ-da da bu problem ölkə mütəxəssisləri, alimləri və təcrübəçiləri tərəfindən geniş tədqiq olunmuşdur. ABŞ-da bu problem son 15 ildə daha çox araşdırılmışdır. Bunu ABŞ rəsmi dairələrinin, Müdafiə Nazirliyinin, Konqresin müxtəlif rəsmi sənədlərində, rəsmi şəxslərin açıq bəyanatlarında, informasiya müharibəsi problemləri ilə məşğul olan təşkilatların hesabatlarında görmək mümkündür.

İM üzrə mütəxəssis Martin Libiki bildirir ki, informasiya müharibəsi Pentaqonda daim gündəmdə olan mövzudur və müharibənin gələcəyini düşünmək qaçınılmazdır. Pentaqonun rəhbərlərindən biri demişdir: "Biz inkişafın elə bir həddinə yaxınlaşırıq ki, burada heç kim əsgər deyil, lakin hamı döyüş iştirakçısıdır. Artıq vacib olan məsələ canlı qüvvənin məhv edilməsi deyil, əsas məsələ əhalinin dünyaya baxışının, məqsədlərinin sarsıdılmasıdır, sosiumun dağıdılmasıdır"[8].

M.Libiki "İnformasiya müharibəsi nədir?" məqaləsində İM-nin 7 formasını təsnifatlaşdırmış, "Information Warfare" ("İnformasiya müharibəsi") adlanan bu sistemdə texnologiyalar arasındakı əlaqələri şərh etmişdir. Bu texnologiyalara, əsasən, komanda-nəzarət, kəşfiyyat, elektron, psixoloji, xaker, iqtisadi, kibermüharibəaid edilir:

1. Komanda-nəzarət müharibəsi(Command and Control Warfare) - komandanlıq və icraçılar arasındakı əlaqə kanallarına yönəlmiş İM-dir. Bu əlaqə kanallarının hər hansı funksiyası pozularsa, İM-də qələbənin təmin olunması reallaşmış olar. Komanda nəzarət müharibəsində "antinik" (anti-neek) adlanan

əməliyyatlara daha böyük önəm verilir ki, bunun da mənası lazımsız, avara müdaxilələrə qarşı tədbirlər deməkdir.

2. Kəşfiyyat müharibəsi(Information Based Warfare) - mühüm informasiyaların toplanması və bu zaman hücum edən tərəfin öz informasiya resurslarını mühafizə etməsi prosesidir.

3. Elektron müharibə(Electronic Warfare) - elektron kommunikasiya texnologiyalarına qarşı yönəlmiş informasiya müharibəsidir. Elektron kommunikasiya texnologiyaları dedikdə, radioəlaqə, radarlar, kompyuter şəbəkəsi nəzərdə tutulur. Onun əsas bölməsi isə kriptoqrafiya (elektron informasiyanın şifrələnməsi və ya şifrədən çıxarılması) hesab olunur.

4. Psixoloji müharibə(Psychological Warfare) - təbliğat, "beyinlərin yuyulması", əhalinin davranışlarına nəzarət etmək və vətəndaşlar üçün nəzərdə tutulmuş informasiyanın emalıdır. M.Libiki psixoloji müharibənin 4 formasını qeyd etmişdir: 1) Vətəndaş ruhunun sarsıdılması; 2) Hərbi qüvvələrdə mənəvi duruma və əhval-ruhiyyəyə nəzarət; 3) Komandanlığa dezinformasiyanın ötürülməsi; 4) Mədəniyyətlərin müharibəsi (War of Culture).

5. Xaker müharibəsi (Hacker Warfare) - qarşı tərəfin mülki obyektlərinə yönəlmiş diversiya əməliyyatlarıdır. M.Libiki xaker fəaliyyətlərindən söz açarkən onların törətdiyi fəsadları belə sadalayır: şəbəkənin total iflici, informasiya əlaqələrində fasilələr, verilənlərin ötürülməsi zamanı təsadüfi səhvlərin çoxalması, informasiyanın oğurlanması, informasiya xidmətlərinin ələ keçirilməsi (şəbəkəyə icazəsiz müdaxilə), şəbəkənin gizli monitorinqinin aparılması, şantaj məqsədi ilə gizli verilənlərin aşkar edilməsi. M.Libikiyə görə, xakerlərin silahı "troyan atları", məntiqi bombalar, sniferlər (izləyiçilər), şəbəkə soxulcanları və s kimi viruslardır.

6.İqtisadi informasiya müharibəsi(Economic Info-Warfare) - M.Libiki bu müharibənin iki formasını təsvir edir: informasiya blokadası (ABŞ-a qarşı yönəlmiş) və informasiya imperializmi və ya texno-imperializm (ABŞ tərəfindən). İnformasiya blokadası dedikdə, ilk sırada, informasiya və ticarət əlaqələrinin kəsilməsi (fiziki ticarətə qadağanın qoyulması) nəzərdə tutulur. Bank şəbəkələrinin sındırılması bu kateqoriyaya aid edilmir və xaker fəaliyyəti hesab olunur. İnformasiya imperializmi

ümumi iqtisadi imperializm siyasətinin tərkib hissələrindən biridir. M.Libiki qeyd edir ki, ticarətin özü də müharibədir.

7. Kibermüharibə (Cyberwar) fəaliyyətini analiz edərkən M.Libiki onu adi xaker müharibəsindən fərqləndirir. Mütəxəssisin fikrincə, əgər nəzərə alınsa ki, terrorizm ayrı-ayrı insanlara və ya təşkilatlara qarşı müharibədir, demək, informasiya terrorizmi isə hədəfi təyin etmək və ya şantaj üçün bir vasitədir. İnformasiya terrorizminin əsasını semantik hücumlar təşkil edir. M.Libiki semantik hücumları təhlil edərkən onları xaker müharibələrindən tam fərqləndirir və qeyd edir ki, əgər xaker müharibəsində xakerin məqsədi sistemin normal fəaliyyətini pozmaqdan ibarətdirsə, semantik hücumlar sistemin fiziki göstəricilərinə və kompyuterin normal işini təmin edən obyektlərə qarşı yönəlir. Sistemin fiziki göstəricilərini və ya digər giriş vasitələrini "aldatmaq" sistemə heç bir texniki zərər vurmadan onu sıradan çıxarmaq deməkdir[1, 84-86].

Müasir İM-də əməliyyatlar iki üsulla aparılır: informasiya-texniki təsir və informasiya-psixoloji təsir.

İnformasiya-texniki təsir– müxtəlif növ informasiya sistemlərinə (verilənlər bazası, verilənlər bankı, analitik sistemlər və s.), telekommunikasiya vasitələrinə, kompyuter şəbəkəsinə və s. texniki vasitələrə təsirdir. İnformasiya-texniki təsir dedikdə, radioelektron mübarizə, radioelektron kəşfiyyat, kompyuter şəbəkələrinə müdaxilə, haker müharibələri və s. nəzərdə tutulur. Texniki obyektlər kimi əlaqə və idarəetmə sistemləri, dövlətin maliyyə-iqtisadi fəaliyyətli və s. hədəfə alına bilər.

İnformasiya-psixoloji təsir– siyasi elita və əhalinin psixoloji durumuna, davranışına, cəmiyyətin informasiya-psixoloji mühitinin inkişafına, funksionallığına birbaşa təsir göstərən xüsusi informasiyanın məqsədəuyğun istehsalı və yayılmasıdır. Təbliğat, "beyinlərin yuyulması" və psixoloji təsir informasiya-psixoloji təsirin növləridir. İnformasiya-psixoloji təsir zamanı hansı üsuldan istifadə olunacağı ilk növbədə məqsəd və hədəflərin düzgün təyinindən asılıdır [22, 223].

İM-də əməliyyatlar əsas iki istiqamətdə aparılır – informasiya hücumu və informasiya mühafizəsi:

1. İnformasiya hücumu (Information Attack) – qarşı tərəfin informasiya infrastruktrunun tam məhv edilməsi və ona öz qüvvəsindən istifadə imkanı verməməkdir. Burada informasiya hücumunun hədəfi kimi dezinformasiya, radioelektron vəsaitlərin, informasiya bazalarının məhvi, qarşı tərəfin kompyuter şəbəkəsinə hücum və s. daxildir. Bu sırada qarşı tərəfin elektron informasiya bazalarının kiberməhvi xüsusi önəm daşıyır. "İM-də informasiya hücumu" dedikdə, şəbəkələrarası birləşmələr vasitəsi ilə informasiya hesablama şəbəkələrinə təsir, şəbəkədə aktiv axtarış, icazəsiz fəaliyyət və nəhayət, informasiya qarşıdurması nəzərdə tutulur.

2. İnformasiya mühafizəsi(Information Protection) – obyektin öz məlumatlarının və inforamasiya strukturlarının əks tərəfin təsirlərindən mühafizəsi nəzərdə tutulur. Buraya informasiyanın strateji maskalanması, informasiya infrastruktrunun fiziki qorunması, dezinformasiya, radioelektron mübarizə və s. daxildir. İM-in mühafizə hissəsi təhlükəsizliyin təminatı metodları ilə realizə olunur [22, 219].

"Şəbəkə müharibəsi" (Network War) terminindən ilk dəfə 1993-cü ildə Con Arkuilla (John Arquilla) və Devid Ronfeldt (David Ronfeldt) tərəfindən "Kiber müharibə gəlir!" (Cyber War Is Coming!) məqaləsində istifadə edilmişdir. Müəlliflər məqalədə kibernetik və şəbəkə müharibəsi konsepsiyalarını (Network Centric Warfare - NCW) irəli sürməklə, müasir dövrdə informasiya müharibəsinin təsəvvür ediləndən də ciddi problemlər yaratmaq imkanına malik olduğunu göstərdilər[33, 84-86].

İnformasiya müharibəsi münaqişənin elə növlərindən biridir ki, burada rəqibin biliklərinə, ehtimallarına təsir göstərilir, lazım gəldikdə, rəqibin informasiya sisteminə birbaşa hücumlar edilir.

İnformasiya müharibəsi bir çox səbəbdən sürətlə yayıla bilər. Bu səbəblərdən beşini xüsusilə qeyd etmək lazımdır:

1. İnformasiya texnologiyalarının sürətlə yayılması və nisbətən ucuz olması, qeyri-dövlət aktorlarının, mafiya təşkilatlarının, terror qruplarının, hətta

müstəqil fərdlərin və kiçik dövlətlərin də informasiya müharibəsi dövrünə keçməsini getdikcə daha da asanlaşdıracaq;

2. İnformasiya müharibəsi barəsində hələ də konkret bir hüquqi tənzimləmə yoxdur. Beynəlxalq müqavilələrin olmaması onu daha da təsirli hala gətirmişdir;

3. Bu sahədə beynəlxalq müqavilələrin olmaması digər, üçüncü bir təhdid ünsürünün meydana çıxmasına səbəb olur: psixologiyaya, duyğulara mənfəət və seçimlərə təsir edə biləcək yeni texnologiyaların yaranması;

4. İnformasiya müharibəsində hücumların inkişaf sürəti o qədər yüksəkdir ki, böhranların dərinləşməsinə belə imkan vermir;

5. Əvvəllər hər kəsə açıq olmayan informasiyanın artıq hamı üçün əlçatanolması.

İnformasiya müharibəsində mübarizə aparan tərəflər öz istəklərini reallaşdırmaq məqsədilə bir-birilərinin informasiya və intellektual sahələrinə təsir edə biləcək bütün vasitələrdən istifadə etməyə çalışırlar. Bu zaman informasiya müharibəsinin 3 ən əsas məqsədini qeyd etmək olar:

1. İnformasiya məkanına güclü nəzarət etmək, ondan səmərəli şəkildə faydalanmaq, eyni zamanda da öz informasiya funksiyalarımızı qarşı tərəfin hücumlarından müdafiə etmək (kontrinformasiya);

2. Öz informasiya məkanını nəzarətdə saxlayaraq qarşı tərəfə yönəlik informasiya hücumlarından istifadə etmək;

3. İnformasiya funksiyalarından istifadə edərək hərbi qüvvələrin effektivlik dərəcəsini maksimuma yüksəltmək [6].

Məqsədyönlü informasiya təsirinə məruz qalan obyektlərə uyğun olaraq informasiya hədəflərini 4 qrupaaid etmək olar: 1. Qərarların qəbul edilməsi və idarəetmə sistemləri (idarə strukturları, kommunikasiya vasitələri); 2. Mülki informasiya infrastrukturu (telekommunikasiya sistemləri, nəqliyyatın, energetikanın, maliyyənin, informasiya sistemləri); 3. Hərbi informasiya infrastrukturu (nəzarət, idarə və əlaqə sistemləri, kəşfiyyat aiddir); 4. Sosial sahələr (insanların psixologiyası, davranışları və əxlaqi stereotiplər, ayrı- ayrı şəxslər və s.)[1, 86-87].

Beynəlxalq mühitin getdikcə mürəkkəbləşməsi, yeni maraqların yaranması ölkələrin yeni strateji hədəflər müəyyənləşdirməsinə səbəb oldu. Beləliklə, hər ölkə öz mənfəətləri üçün yeni strateji hədəflər formalaşdırmağa başlamışdır. Bu hədəflərin sırasında çox keçmədən informasiya müharibələri də yer almış və XXI əsrdə yeni bir anlayış "strateji informasiya müharibəsi" termini meydana gəlmişdir.

Strateji informasiya müharibəsi, ölkənin strateji hədəflərinin nəzərə alındığı və ənənəvi strateji müharibə anlayışından fərqli olaraq, informasiya texnologiyaları vasitəsilə milli informasiya bazasını və bu bazayla əlaqəli olan nöqtələri çökdürmək məqsədilə həyata keçirilən müharibə kimi təsnif olunur.

Strateji informasiya müharibəsinin meydana gəlməsi üçün iki fərqli bucağın birləşməsi lazımdır. Bunlardan birincisi ölkənin sahib olduğu informasiya texnologiyaları və kiber kosmos bazası; digəri isə o ölkənin ərtafında cərəyan edən beynəlxalq siyasi mühitlə bağlı olan vəziyyətlərdir [22, 220].

Strateji informasiya müharibəsi anlayışını daha yaxşı başa düşmək üçün Molender və Riddlenin bu çərçivədə müəyyənləşdirdiyi 7 əsas xüsusiyyətə nəzər yetirmək lazımdır.

1. Xərclərin daha az olması.Ənənəvi hərbi texnologiyalardan fərqli olaraq, informasiya texnologiyaları inkişaf etdirildiyində həddən artıq çox maliyyə qaynağına və ya dövlətin maddi yardımına ehtiyac qalmır.

2. Ənənəvi sərhədlərin naməlum olması. Bu xüsusiyyət, strateji informasiya müharibəsi üçün coğrafi, bürokratik, hüquqi və konseptual mənada yeni problemlər ortaya çıxarmışdır. Strateji informasiya müharibəsinin reallaşdığı təqdirdə bu problemin mövcudluğundan söz gedə bilməz. Çünki artıq tərəflər arasında əlaqələrin etibarlılığı aradan qalxır və anlaşılmazlıqlar nəticəsində müharibə baş verir.

3. Qavrayış idarəolunmasının genişlənməsi və yeni rollar. Texnologiyaya əsaslanan yeni informasiya, yanıtlmanın gücünü, görüntülü manipulyasiyanı, təhlükəsizlik üçün dövlətin verdiyi dəstəyi həddindən artıq çətinləşdirə bilər. Bu məqsədlə dövlət və qeyri-dövlət aktorlarının qavrayışlarının müharibə psixologiyasına uyğunlaşdırılması zərurəti ortaya çıxır.

4. Yeni strateji kəşfiyyat modellərinin yaranması. Qarşı tərəfdəki düşmənin niyyətini anlamaq və gücünü müəyyən etmək məqsədilə aparılan strateji kəşfiyyat, klassik kəşfiyyatın əhatə dairəsini məhdudlaşdırmışdır. Bundan əlavə dövlətlər, özlərinə qarşı yönələn təhdidlərin təbiətinin sürətlə dəyişməsinin nəticəsi kimi, istər coğrafi, istərsə də virtual mühitdə öz yerlərinin müəyyən edilməsində çətinliklərlə üzləşirlər. Bu çətinliyi aradan qaldırmaq üçün yeni kəşfiyyat modellərinin işlənib hazırlanması lazımdır.

5. Taktiki xəbərdarlıq və hücumların başa düşülməsinin çətinliyi. Strateji informasiya müharibəsində, taktiki xəbərdarlıq və hücumların təsbit edilməsi həddən artıq çətindir.

6. Koalisiyaların yaranması və davamlılığının çətinliyi. Strateji informasiya müharibələri nəticəsində, dövlətlərin hər hansı qarşıdurma vəziyyətində istər regional, istərsə də beynəlxalq koalisiyaya daxil olması çətinləşmişdir.

7. ABŞ-ın hücumlara məruz qala bilmə ehtimallarınınyüksək olması.ABŞ-ın hegemon güc kimi hücuma məruz qala bilmək ehtimalının yüksək olması onu kiber kosmos sahəsində daha sürətli inkişafa nail olmağa sövq etmişdir. Bu səbəbdən, ABŞ 2002-ci il büdcəsindən 2,7 mlrd dollar, 2003-cü il büdcəsindən isə 4,2 mlrd dollar "virtual təhlükəsizlik xərcləri" üçün ayırmışdır[58].

ABŞ-da 2006-cı ildən başlayaraq ölkənin hərbi-siyasi rəhbərlərinin iştirakı ilə "İnformasiya müharibəsi" üzrə elmi konfranslar keçirilməyə başlanılmışdır. ABŞ-ın Ohayo şəhərində yerləşən Hərbi Hava Qüvvələrinin Texniki Universitetində 2010-cu ilin aprel ayında 5-ci konfrans (5th International Conference on Information Warfare and Security) keçirilmişdir[1,89; 87].

Nəticə etibarilə qeyd etmək lazımdır ki, informasiya müharibələri dünya dövlətlərinin diqqət mərkəzində olan əsas məsələ və buna qarşı mübarizə XXI əsr dünya dövlətləri qarşısında duran əsas vəzifələrdəndir. Qeyd olunduğu kimi, "İnformasiya Müharibəsi" anlayışı ilk dəfə ABŞ-da meydana gəldi və daha geniş şəkildə məhz bu məkanda araşdırıldı. Bu isə İnformasiya Kommunikasiya Texnologiyalarının ABŞ-da geniş şəkildə inkişafı və tətbiqi ilə əlaqədardır. İnformasiya müharibəsi üzrə mütəxəssis Martin Libiki bu müharibənin əhəmiyyətini

xüsusilə qeyd etmiş və müharibənin gələcəyi haqqında düşünməyin qaçınılmaz olduğunu vurğulamışdır. M. Libiki ilk dəfə bu müharibənin 7 əsas formasını təsnifatlandırmış və müharibədə istifadə olunan texnologiyalar arasındakı əlaqələri göstərmişdir. Qeyd olunan təsnifata əsasən, bura komanda-nəzarət, kəşfiyyat, elektron, psixoloji, xaker, iqtisadi və kiber müharibələr aiddir.

1.2. İnformasiya təhlükəsizliyinin təmin olunması sahəsində federal qanunvericilik

ABŞ milli informasiya təhlükəsizliyinin təmin olunması üçün mərkəzi təşkilat yaratmaq əvəzinə, koordinatorlar vətəcrübəçilərin koordinasiyasıyla idarə olunan təşkilat modelini seçmişdir. ABŞ-da mühüm infrastrukturların qorunması da daxil olmaqla, hər sahə üzrə birdən çox təşkilat mövcuddur və bu təşkilatların hər birinin bir sıra fərqli rolu vardır. 2002-ci ildə Konqres tərəfindən "Vətənpərvərlik Aktı" (Patrist Act) qəbul edilmiş vəbununla daDaxili Təhlükəsizlik Nazirliyi (Departiment of Homland Security-DSS) yaradılmışdır. Eyni zamanda bu nazirliyin nəzdində də Milli Kiber Təhlükəsizlik Bölməsi (National Cyber Security Division) yaradılmışdır. Milli informasiya təhlükəsizliyi strategiyasının koordinasiyasında Elm və Texnologiya Siyasəti Ofisi (Office of Science and Technology Policy-OSTP), İdarə və Büdcə Ofisi (Office of Management and Budget-OMB), Ədliyyə Nazirliyi (Depertment of Justice -DOJ), Xarici İşlər Nazirliyi (US Department of State-DOS) kimi federal təşkilatların rolu böyükdür. Digər tərəfdən isə strategiyanın tətqiqatçıları kimi həm ictimai həm də özəl sektordakı təşkilat və qurumların rolu da kifayət qədərdir. Xüsusilə mühüm infrastrukturların qorunması ABŞ-ın əhəmiyyətli strateji piroritetləri sırasında yer almışdır. Bununla əlaqədar "İnformasiya Dövründə Mühüm İnfrastrukturların Müdafiəsi" (Critical infrastructure Protection in the information Age) adlı Prezident Drektivi mühüm infrastrukturların müdafiəsi ilə bağlı təşkilatların, qurumların vəzifə və səlahiyyətlərini müəyyənləşdirmişdir [16, 75].

ABŞ Konqresi ötən 200 il ərzində daima informasiya siyasətini diqqət mərkəzində saxlamışdır[52, 175]. Konqresə görə iqtisadi, siyasi, və mədəni sferada iştirak etmək, informasiya xidmətlərinə çıxış və bu xidmətlərdən istifadə ilə sıx bağlıdır [60, 236;12, 596].

Konqres, kompüterlərin və internetin vətəndaşlar, xüsusi müəssisələr və hökumət arasındakı əlaqələri dərindən dəyişdiyini, federal hökumətin funksiyalarını və xidmətlərini artırmaq üçün informasiya texnologiyalarının tətbiqində qeyri-bərabər müvəffəqiyyət əldə olunduğunu aydınlaşdırdı. İnternetdən və elektron hökumətin xidmətlərindən istifadəni genişləndirmək və federal hökumətin daha şəffaf hesabat verə bilməsi üçün 2002-ci ildə "E-dövlət Aktı" (E-Government Act) qəbul olundu. Bu qanun məxfiliyin qorunması, milli təhlükəsizlik və digər bu kimi qanunlarla əlaqələndirilmişdi [40].

Konqresdə müzakirə olunan və prezident tərəfindən 2002-ci ilin dekabrında imzalanan E-Dövlət Aktında (Public Law 107-347) informasiya təhlükəsizliyinin Birləşmiş Ştatların iqtisadi və milli təhlükəsizlik maraqları ilə birbaşa bağlılığığz əksini tapmışdı. E-Dövlət Qanununun, Federal İmformasiya Təhlükəsizliyi İdarəetmə Aktı (Federal İnformation Security Management Act-FİSMA) adlanan 3-cü başlığı, hər bir federal agentliyin əməliyyatlarını, aktiv fəaliyyətini dəstəkləyən, informasiya sistemlərinin təhlükəsizliyini təmin etmək üçün agentlik səviyyəsində proqram yaradılmasını, onun tətbiq olunması və hesabatların hazırlanmasını tələb edir. Digər qaynaqlar tərəfindən təmin edilən və ya idarə olunan proqramlar da agentliyin səlahiyyətlərinə daxildir [42].

Qanunun məqsədlərinə federal əməliyyatları dəstəkləyən informasiya mənbələrinin üzərində, informasiya təhlükəsizliyi idarələrinin fəaliyyətini tam şəkildə təmin etmək; ölkə səviyyəsində, informasiya təhlükəsizliyi riskləri mövzusunda maraqlı olan tərəflərin əməkdaşlığına, koordinasiyasına nail olmaq və onlara nəzarəti təmin etmək; federal informasiya sistemlərini qorumaq üçün lazım olan kiçik idarələrin inkişaf etdirilməsi və onların baxımı üçün dəstəyi təmin etmək;Federal informasiya təhlükəsizliyi proqramlarının nəzarəti üçün infrastruktur yaratmaq daxildir [26, 10].

Qanunun anlayışlar hissəsində “informasiya təhlükəsizliyinin qorunması” anlayışının mahiyyəti açıqlanmış,onun bütünlük, gizlilik, əlyetənlik və identifikasiya xüsusiyyətləri qeyd olunmuşdur. Qanuna görə hər bir federal təşkilat öz fəaliyyətinə təsir edən informasiya sistemlərinin təhlükəsizliyini təmin etməlidir. Federal təşkilatlar informasiya sistemlərinə icazəsiz giriş, istifadə etmə, ifşa etmə, pozma, dəyişdirmə və yox etmə fəaliyyətləri nəticəsində ortaya çıxa biləcək zərərləəlaqəli olan riskləri analiz etmək; informasiya sistemlərinin davamlılığı üçün lazımlı işlər görmək; təhlükəsizlik üçün lazım olan prinsip və prosedurları inkişaf etdirmək; işçiheyətinin maarifləndirmə səviyyəsini artırmaq üçün tədbirlər görmək; il ərzində keçirilən tədbirlərin fəaliyyətini və performansını qiymətləndirmək; keçirilən tədbirlərin xərci ilələlaqədar analizlər etməkkimi vəzifələri yerinə yetirməlidirlər[26, 10].

FİSMA 1995-ci ildə qəbul olunan Sənədləri Azaltma Aktı və 1996-cı il tarixində qüvvəyə minən İnformasiya Texnologiyası İdarəsi və İstehsalı Aktı (Clinger-Cohen Act) ilə birlikdə, informasiya təhlükəsizliyinə olan hədələrin və risklərin aradan qaldırılması üçün tövsiyyələr vermişdir.Qanunda göstərilir ki, agentliklər, proqram səlahiyyətliləri, informasiya məhsulları və informasiya təhlükəsizliyinin təmin edilməsi üçün hazırlanan proqramların gördüyü işin nəticələrini İdarə və Büdcə Offisinə (Office of Management and Budget) təqdim etməlidir. İdarə və Büdcə Offisi isə bu informasiyaları illik hesabat şəklində hazırlayıb Konqresə təqdim edir. 2008-ci ildə federal təşkilatlar informasiya texnologiyalarının təhlükəsizliyi üçün ümumilikdə 6,2 milyard dollar vəsait istifadə etmişdilər [42].Bu qanunu dəstəkləmək və fəaliyyətini gücləndirmək üçün İdarə və Büdcə Ofisindən və federal hökumət daxilində mövcud olan icra hakimiyyəti orqanlarından bunları etmək tələb olunur: təhlükəsizlik planının hazırlanması; uyğun səlahiyyətlilərə təhlükəsizliyi təmin etmək üçün vəzifələrin verilməsi; təhlükəsizlik sistemlərinin periodik olaraq yoxlanılması; keçirilən əməliyyatlardan əvvəl və sonra periodik olaraq sistemlərin işləməsinə icazə verilməlidir.

Qanuna əsasən agentliklər bu sahədə məsuliyyətli olan əməkdaşlarının işinə mənfi təsir edə biləcək riskləri və digər faktorları tam dərk etməlidirlər. Bundan

əlavə, bu səlahiyyətlilər həm də təhlükəsizlik proqramlarının mövcud vəziyyəti, təhlükəsizlik tədbirləri, mövcud riskləri qısa müddətdə aradan qaldırmaq üçün əvvəlcədən alınmış qərarlar və investisiya yatırmaq üçün əvvəlcədən seçilmiş yerlərlə tam tanış olmalıdırlar. Əsas hədəf isə agentliyin gündəlik əməliyyatlarını icra etmək, tapşırılan vəzifələri kifayət qədər təhlükəsiz və risklərin olmadığı şəraitdə yerinə yetirməkdir.

Artmaqda olan riskləri aradan qaldırmaq üçün federal təhlükəsizlik tətbiqlərini modernizə edən və müxtəlif dəyişikliklər gətirən 2014-cü ilin "Federal İmformasiya Təhlükəsizliyi Modernizasiya" Aktı, 2002-ci ildə qəbul olunmuş"Federal İmformasiya Təhlükəsizliyi İdarəetmə" Aktına dəyişikliklər etdi. Bu dəyişiklər nəticəsində, daha az ümumi hesabatlar hazırlanması, sistemlərdə davamlı olaraq nəzarətin gücləndirilməsi, agentliklərə uyğunlaşdırılması vətəhlükəsizliyə olan təhdidlərin səbəb olduğu mövzulara daha çox diqqət yetirilməsi nəzərdə tutulmuşdur.

Bu qanuna 2014-cü ildə 5 əsas dəyişiklik edildi:Federal Təhlükəsizlik Sistemləri Dairəsi katibi digər agentliklərə informasiya təhlükəsizliyi iləəlaqəli bütün işlərdə yardım etməlidir; Siyasi və maliyyə sahələrində informasiya təhlükəsizliyinə təhdidlər göstərilməlidir; Hər hansı bir agentlikdə informasiya təhlükəsizliyinə aid pozuculuq halı baş verərsə,ən gec 30 gün müddətində İdarə və Büdcə Ofisi bu haqda Konqresə xəbər verməlidir;İdarə və Büdcə Ofisi A+130 proqramını yeniləməlidir; Agentliklərin başçıları texniki yardımla təmin edilməlidir[54].

Təhlükəsizlik və gizliliyin təmin olunması iləəlaqədar olaraq, yenilənmiş A-130 proqramı, federal təşkilatlarda təhlükəsizliyin və gizliliyin qorunması zərurətini vurğulayır, strateji və davamlı risklərin qarşısının alınması proqramına keçidi təmsil edir [54].

FİSMA nəşrləri, Federal İnformasiya Təhlükəsizliyi Modernizasiya Aktının təyin etdiyi vəzifələrə uyğun olaraq NİST (National İnstitute of Standarts and Technology) tərəfindən yayınlanmışdır. NİST-in əsas vəzifəsi federal sistemlərin minimum tələbləri də daxil olmaqla, informasiya təhlükəsizliyi standartlarını inkişaf etdirməkdir [65]. Lakin bu standartlar və təlimatlar səlahiyyətli nümayəndələrin təsdiqi olmadan milli təhlükəsizlik sistemləri üçün etibarlı deyil [42]. Eyni zamanda

federal informasiya sistemlərinin təhlükəsizliyini daim nəzarət altında saxlamaq da NİST-in səhaliyyətlərinə daxildir[84, 6-12].

NİST bu qanun layihəsinin agentliklər tərəfindən əhatəli və balanslı şəkildə tətbiq olunması üçün inteqrativ "Risk İdarə Çərçivəsi" (Risk Management Framework) proqramını irəli sürmüşdür [45, 5-17].

ABŞ-da 1988-ci ilyanvarın8-də keçirilən 100-cü Konqresdə də informasiya təhlükəsizliyi məsələsinə xüsusilə toxunulmuşdur. Bu Konqresdə informasiya təhlükəsizliyinə aid qəbul olunan qanun "1987-ci ilin Kompüter təhlükəsizliyi Aktı" (Computer Security Act of 1987) adlanır. Konqresdə müzakirə olunan əsas məsələlərdən biri də standart kompüter proqramlarının yaradılması ilələlaqədar olmuşdur. Qanunda qeyd olunmuşdur ki, informasiya infrastrukturunun qorunması, onun daha yaxşı müdafiə olunması üçün xüsusi standartlı komputer proqramları yaradılmalıdır. Belə proqramların yaradılması, ABŞ-ın texnoloji cəhətdən yüksək inkişafına da töhfə vermiş olacaq[88,1724-1728].

1996-cı il fevralın10-da keçirilən 104-cü Konqresdə qəbul olunan "İctimai qanun"un (Public Low) ikinci başlığı informasiya təhlükəsizliyinə həsr olunmuşdur. Konqresdəmüzakirə olunan məsələlərdən biri "İnformasiya texnologiyalarının satın alınması və pilot proqramları" haqqında olmuşdur. Sənəddə vurğulanır ki, informasiya texnologiyalarının satın alınması ölkənin iqtisadi inkişafına yardım edəcək, eyni zamanda da informasiya təhlükəsizliyinin qorunmasına kömək edəcək. Sənəddə pilot proqramları haqqında da qeyd olunmuşdur. Pilot proqramlarının iki növü fərqləndirilir: 1. Qənaət məqsədli pilot proqramları; 2. Problemlərin həll edilməsinə yönəlmiş pilot proqramları. Bu proqramların həm yaradılması, həm də digər ölkələrə satılması nəzərdə tutulmuşdur [89, 689-695].

ABŞ-da 2003-cü il yanvarın 3-də fəaliyyətə başlayan 108-ci Konqresdə də informasiya təhlükəsizliyi məsələsinə toxunulmuşdur. Konqresdə NİST-in fəaliyyəti xüsusilə qeyd olunmuşdur. Qəbul olunan qanunda bildirilir ki, NİST informasiya təhlükəsizliyinin təmin olunması sahəsində böyük rola malikdir. İnformasiya sistemlərinin idarə olunması və onların təhlükəsizliyinə nəzarət NİST-in

səlahiyyətlərinə daxildir. NİST informasiya sistemlərinin davamlı olaraq işlək vəziyyətdə olmasına diqqət yetirir [90, 48-63].

2012-ci il, fevralın14-də keçirilən 112-ci Konqres "Kiber və informasiya təhlükəsizliyini təmin etmək üçün infrastrukturların möhkəmləndirilməsi" mövzusunda müzakirələr aparılmışdır. Bu sənəd "2012-ci il Kiber təhlükəsizlikqanunu" kimi də tanınır. Sənəddə qeyd olunur ki, hər bölməyə görə kiber risklər ayrı-ayrılıqda qiymətləndirilməli, onlara uyğun həll yolları göstərilməlidir. Eyni zamanda, mühüm infrastrukturlar müəyyənləşdirilməli və onların təhlükəsizliyinə xüsusi diqqət yetirilməlidir. 2012-ci il Kiber Təhlükəsizlik Aktında vurğulanır ki, mühüm infrastrukturların sahibləri, Mühüm İnfrastruktur Tərəfdaşlığı Məsləhət Şurası və digər federal təşkilatlar ilə birlikdə müşavirələrdə iştirak etməlidirlər. Həmin müşavirələrdə kiber təhlükəsizliklə əlaqəli risklərin təcili sürətdə həll olunması lazım olanın müəyyənləşdirilməsi, mühüm infrastrukturların təyin olunması üçün prosedurların təyin edilməsi və kiber təhlükəsizliyin təmin olunması üçün müxtəlif planların hazırlanması nəzərdə tutulmuşdur [91].

İnformasiya texnologiyalarının sürətli inkişafı və bu texnologiyaların ABŞ-da tətbiqi onu informasiya infrastrukturlarının təhlükəsizliyinə nəzarəti gücləndirməyə vadar etdi. XX əsrin sonları XXI əsrin əvvəllərindən etibarən ABŞ-da informasiya təhlükəsizliyinin təmin olunması sahəsində bir sıra yeni qanunlar işlənib hazırlandı. Bununla əlaqədar olaraq, 2002-ci ildə E-Dövlət Aktının 3-cü başlığı kimi Federal İnformasiya Təhlükəsizliyi Modernizasiya Aktı qəbul olundu. ABŞ-ın Milli Texnologiyalar və Standartlar İnstitutu bu qanunun tətbiq olunmasına xüsusi diqqət yetirir. Bu institut həmçinin informasiya təhlükəsizliyinin təmin olunması üçün hər il müxtəlif hesabatlar hazırlayır.

1.3.ABŞ-da informasiya müharibələri haqqında konsepsiyaların təkamülü

İnformasiya texnologiyalarının inkişafında kifayət qədər uğur qazanan ABŞ, həm də informasiya təhdidləri ilə ən çox üzləşən ölkədir. Bu çərçivədə, ABŞ-ın milli informasiya sistemlərinin və infrastrukturlarının təhlükəsizliyini təmin etmək sahəsində gördüyü tədbirlər 1990-cı illərin birinci yarısına qədər gedib çıxmışdır. Bu dövrdə başlayan və sonrakı illərdə ABŞ üçün real milli təhlükəsizlik təhdidi kimi formalaşan kiber təhlükəsizlik hadisələri, ABŞ-ın bu sahədə təhlükəsizlik strategiyasınıformalaşdırmaq zərurətini ortaya çıxartmışdır. 2001-ci il 11 sentyabr terror hadisəsindən sonra bu məsələyə ölkə tərəfindən daha da ciddi yanaşıldı. Artıq ölkənin informasiya və təhlükəsizliklə bağlı olan strukturlarında, bununla əlaqədar olaraq, yeni təşkilatlar formalaşmağa başladı. Bu təşkilatların təhlükəsizliklə bağlı üzərinə götürdüyü öhdəliklər sırasında milli informasiya təhlükəsizliyinin təmin edilməsi ön sırada dururdu.

2001-ci il 11 sentyabr hadisələrindən dərhal sonra Milli Təhlükəsizlik Strategiyası (National Security Strategy) qəbul olundu. Bu strategiyabaşqa adla "Buş Doktrinası" da adlanır. Strategiya 9 bənddən ibarətdir. Bəndlərə nəzər saldıqda, ABŞ-ın Beynəlxalq Strategiyasına baxış, qlobal terrorizmə qarşı mübarizədə ittifaqların gücləndirilməsi, regional münaqişələrin həllində müttəfiqlər ilə birlikdə çalışmaq, düşmənlərə, hədələrə qarşı qabaqlayıcı tədbirlər görmək və s. kimi məsələlərə diqqət yetirildiyinin şahidi olmaq olar [80, 35].

İlk baxışda strategiyanın heç bir bəndində informasiya təhlükəsizliyi məsələsinə toxunulduğu görünmür. Lakin informasiya təhlükəsizliyinin nə qədər önəmli faktor olduğu düşünüldüyündən bu srategiyanın tərkib hissəsi kimi 2003-cü ildə "Kiber Məkanın Təhlükəsizliyi üçün Milli Strategiya" (The National Strategy to Secure Cyber Space) adlı sənəd qəbul olundu.

Kiber məkandan istifadə edərək həyata keçirilənterror hücumlarının ölkənin mühüm infrastrukturlarına göstərdiyi təsir, ABŞ-ın informasiya təhlükəsizliyi

sahəsində kiber təhlükəsizliyə xüsusi diqqət yetirməsinə səbəb olmuşdur. Bununla əlaqədar olaraq, 2003-cü ildə ilk milli strategiya kimi “Kiber Təhlükəsizliyi Təmin Edən Milli Strategiya” (National Strategy to Secure Cyber Space) tamamlanaraq qüvvəyə minmişdir. ABŞ-ın milli informasiya təhlükəsizliyi strategiyası kimi xarakterizə edilən bu sənəd, 11 sentyabr hadisələrindən dərhal sonra hazırlanan Milli TəhlükəsizlikStrategiyasının bir komponenti olaraq nəzərdə tutulmuşdur. İnternetdə mövcud olan bütün risklərə və təhdidlərə baxmayaraq o, ABŞ üçün əvəzsiz bir texnologiya xüsusiyyəti daşıyırdı. Bütün federal səviyyədəki qurum və təşkilatlara, özəl sektor təşkilatları və fərdlərə aid informasiya sistemləri bu mühit vasitəsilə bir-biri ilə əlaqə saxlayır, xidmət infrastrukturlarında mübadilələr həyata keçirir və bu xidmətlərdən gəlir əldə edirdi. Kiber mühitin təhlükəli vəziyyətdə olması, milli təhlükəsizliyə olduqca ciddi risk kimi qəbul edildiyindən, milli informasiya təhlükəsizliyi strategiyası formalaşdırılmışdır[16, 75].

Bu strategiyanın əsas prioritetləri bunlardır:ABŞ-ın mühüm informasiya infrastrukturlarının kiber hücumlara qarşı qorunması;Kiber hücumlara qarşı milli diametrdə mövcud olan bir sıra zəif cəhətlərin aradan qaldırılması;Hər hansı bir kiber hücumun vura biləcəyi ziyanın, mümkün qədər ən az zərərlə və ən qısa müddətdə aradan qaldırılması[82, 8].

Bu strateji hədəflərə çatmaq üçün isə 5 əsas proritetin yerinə yetirilməsi nəzərdə tutulmuşdur:Kiber mühitə təcili müdaxilə etmək üçün milli sistem yaradılması;Kiber mühitin təhlükəsizliyinə təhdidlərin və risklərin azaldılmasına dair milli kontekstdə proqramların hazırlanması;Kiber mühitin təhlükəsizliyini təmin etmək üçün maarifləndirmə və təhsil proqramlarının hazırlığına başlanılması;Milli və beynəlxalq müstəvidə kiber mühitin təhlükəsizliyinin təmin edilməsinə dair əməkdaşlıq işlərinin sürətləndirilməsi.

Milli informasiya təhlükəsizliyinin təmin edilməsi müxtəlif səviyyədə keçiriləcək tədbirlər və cəmiyyətin müxtəlif təbəqələrinin əməkdaşlığı ilə mümkün ola bilər. Bu məqamda, Kiber Təhlükəsizliyi təmin edən Milli Strategiyada, bu sahədə maraqlı olan tərəfləri hərəkətə keçirə bilmək üçün aşağıdakı prinsiplərin reallaşdırılmasının vacibliyi xüsusilə vurğulanmışdır:Milli səviyyədə səylərin

göstərilməsi;Məxfilik prinsiplərinə əməl edərək şəxsiyyət hüquqlarına hörmət edilməsi;Hökümətin sanksiya gücü strategiyasını həyata keçirmək əvəzinə, bazar güclərini dövriyyəyə daxil etməsi;Cavabdehlik və hesabat prinsiplərinin gözlənilməsi;Kiber müqavimətin təmin edilməsi;Orta səviyyəli tətbiq müddətinin olması.

ABŞ-ın Kiber Təhlükəsizlik strategiyasının tətbiqində iki müxtəlif istiqaməti bir-birindən fərqləndirmək mümkündür: koordinasiya vahidləri və tətbiq vahidləri. Strategiyanın tətbiq olunması zamanımüxtəlif əməkdaşlıqlar və təşkilati formalaşma imkanlarından da istifadə edilməsi nəzərdə tutulmuşdur. Strategiyanın tətbiqindən cavabdeh olan mərkəzi təşkilat yaratmaq əvəzinə, dövlət və özəl sektorların tərkibində olan təşkilatlara səlahiyyətlər verərək, onların bu işdə iştirakı təmin edilmişdir. Bu strategiyanın həyata keçirilməsi ilə əlaqədar olaraq, informasiya təhlükəsizliyi sahəsində baş vərən irəliləyişlərin isə hesabat şəklində Məşvərət Şurasınatəqdim edilməsi nəzərdə tutulmuşdur. Adı çəkilən strategiyaya 2009-cu ildən yenidən baxılmalı, həmin dövrün aktual hadisələrinə uyğun tətbiq olunmalı idi. Baş tutacaq yenilənmə ilə əlaqədar göstərilmiş sahələrdə tədbirlərin keçirilməsi nəzərdə tutulmuşdur:Təhlükəsiz ictimai internet şəbəkəsinin yaradılması;Cəmiyyətdə mövcud olan kriminal təşkilatların informasiya sistemlərinə sızma cəhdlərinə qarşı hücumları təsbit edən proqramın yaradılması və yayılması;Milli informasiya təhlükəsizliyi sahələrində Ar-Ge fəaliyyətlərinin dəstəklənməsi; (Ar-Ge -insanın, cəmiyyətin və mədəniyyətin informasiya təcrübəsini artırmaq və bu təcrübələri yeni sahələrə tətbiq etmək məqsədilə sistematik təmələ söykənən yaradıcı işləri əhatə edən proqramdır);Situasiya ilə bağlı məlumatı artırmaq üçün, kiber təhlükəsizliklə əlaqəli əməliyyat mərkəzləri və ictimai təşkilatlar arasındakı əməkdaşlığı gücləndirmək, əlaqələrin möhkəmləndirilməsi;Kiber cəsusluğa, kəşfiyyata qarşı qorunma tədbirlərinin ictimai və özəl sektor səviyyəsində genişləndirilməsi;Müharibə, diplomatiya, terrorla mübarizə, hüquq-mühafizə, kəşfiyyat və daxili təhlükəsizlik əməliyyatları ilə əlaqədar təsnif edilmiş informasiyaların və sənədlərin rəqəmsal mühitdə qorunması;Təhsil və maarifləndirmə fəaliyyətinin genişləndirilməsi;Kiber

daşındırıcılığın artırılması;Mühüm informasiya infrastrukturlarının qorunmasında cəmiyyətin rolunun müəyyən edilməsi[16, 77].

ABŞ-da mühüm infrastrukturların fiziki cəhətdən qorunması üçün digər bir milli strategiya hazırlanmışdır. Buna istinadən hazırlanan "Mühüm infrastruktur və Açar Aktivlərin Fiziki Müdafiəsi üzrə Milli Strategiya"sı (The National Strategy for the Physical Protection of Cricital İnfrastructures and Key Assest) adından da aydın olduğu kimi fiziki müdafiəni əsas götürsə də, strategiyada eyni zamanda kiber təhdidlərə də fiziki təhdidlər qədər toxunulmuşdur. Strategiyada müəyyən edilən əsas məqsədlər aşağıdakılardır:Milli səviyyədə sağlamlıq, idarəçilik, iqtisadi və təhlükəsizliklə bağlı ən mühüm hesab etdiyimiz infrastrukturların təyin olunması və müdafiəsi;Zamanında xəbərdarlıq etmək və təhdid altında olan obyektlərin müdafiəsini təmin etmək;Dövlət və özəl sektorların idarə etdiyi infrastrukturların daha yaxşı qoruna biləcəyi təhlükəsiz, əməkdaşlığa əsaslanan mühit yaratmaq və həmin infrastrukturlarda baş verə biləcək terror hadisələrinin qarşısını almaq [81, 7].

ABŞ prezidenti Barak Obamanın hakimiyyəti dövründə, 2010-cu il, mayın 27-ində Milli Təhlükəsizlik Konsepsiyası qəbul edildi. Konsepsiya ABŞ-ın maraqlarını ifadə edən dörd bölmədən ibarətdir. 2002-ci ildə qəbul olunan Milli Təhlükəsizlik Konsepsiyasından fərqli olaraq, informasiya təhlükəsizliyi məsələsinə dair ayrıca strategiya qəbul olunmamış, kiber təhlükəsizlik adlı bənd bu strategiyanın təhlükəsizlik (security) bölməsinin sonuncu bəndi olaraq öz əksini tapmışdır. Konsepsiyada kiber təhlükəsizlik hissəsində qeyd olunmuşdur: "Kiber təhlükəsizliyə təhdidlər, xalq kimi qarşılaşdığımız ən ciddi milli təhlükəsizlik, ictimai təhlükəsizlik və iqtisadi çətinliklərdən birini əhatə edir. Bizə liderlik etmə və yaratmaq imkanı verən texnologiyalar, pozuculuq və dağıdıcılıq fəaliyyəti ilə məşğul olanları da gücləndirə bilər. Bu texnologiyalar bizim hərbi üstünlüyümüzü təmin edir, lakin digər tərəfdən də hökumətə aid olan şəbəkələrimiz "dəvətsiz qonaqlar" tərəfindən də araşdırılır. Gündəlik həyatımız və ictimai təhlükəsizliyimiz elektrik və elektrik şəbəkələrinə bağlıdır, ancaq potensial düşmən onlara böyük həcmdə zərər vurmaq üçün kiber sahədəki zəif nöqtələrdən istifadə edə bilər. İnternet və e-ticarət bizim iqtisadi rəqabət gücümüzün açarıdır, lakin kiber cinayətkarlar şirkətlərə və

müştərilərinə milyonlarla dollar gəlir gətirirlər. Qarşılaşdığımız təhdidlər, oğrular, mütəşəkkil cinayətkar qruplardan tutmuş, inkişaf etmiş ölkələrə qədər dəyişir. Bu təhdidlərə qarşı mübarizə aparmaq üçün təhlükəsiz, etibarlı və çevik şəbəkələr lazımdır. Bu səbəbdən də, rəqəmsal infrastrukturumuz strateji milli varlıqdır və onu qorumaq,eyni zamanda, məxfiliyi, vətəndaşların hüququnu qorumaq təhlükəsizlik prioritetlərimizdən biridir. Kiber hücumların qarşısını almaq, onları aşkar etmək və onlardan ən qısa zamanda qurtulmağa çalışacağıq".

İnsanlara və texnologiyalara investisiya yatırtmaq. Bu hədəfi həyata keçirtmək üçün, hökumət daxilində və özəl sektorlarla birgə çalışaraq mühüm hökumət, sənaye sistemlərinin və şəbəkələrinin elastikliyini daha yaxşı qoruyacaq, onları inkişaf etdirmək üçün etibarlı texnologiyalar hazırlayacağıq. Bu çətinliklərin öhdəsindən gəlmək üçün ehtiyac duyduğumuz şey innovasiyadır. Yeni kəşflər, ən son araşdırmalar üçün investisiya yatırmağa davam edəcəyik. Kiber təhlükəsizliyin müdafiəsini şüurlu şəkildə genişləndirmək, rəqəmsal oxu-yazı sistemlərinə tam keçidi təmin etmək, dərsliklərimizi yüksək səviyyədə hazırlamaq və XXI əsr üçün rəqəmsal işçi qüvvəsini formalaşdırmaqdan ötrü, əhatəli şəkildə milli kampaniyaya başlamışıq.

Əməkdaşlıqların gücləndirilməsi. Nə hökumət, nə özəl sektor, nə də vətəndaşlar fərdi şəkildə bu çətinliyin öhdəsindən gələ bilmir. Birlikdə çalışdığımız yolları genişləndirəcəyik. Kiber mühitdə təhlükəsizliyi təmin etmək üçün beynəlxalq əməkdaşlığımız möhkəmləndirilməlidir. Kiber hücumları aşkara çıxartmaq və gələcəkdə baş verə biləcək hadisələrə birlikdə cavab tədbiri hazırlamaq üçün hökumət və özəl sektordakı əməkdaşlarla birlikdə milli və beynəlxalq səviyyədə çalışacağıq. Eyniylə təbii fəlakətlər zamanı olduğu kimi əvvəlcədən hazırlanmış plan və qaynaqlara sahib olmalıyıq" [78, 27].

Beş illik fasilədən sonra Obama administrasiyası dövründə, 2015-ci il fevralın 6-da yeni Milli Təhlükəsizlik Konsepsiyası qüvvəyə minmişdir. Hələ 2010-cu ilin mayında Milli Təhlükəsizlik Konsepsiyası qüvvəyə minən zaman Ərəb baharı Yaxın və Orta Şərq ölkələrini tam şəkildə sarsmamış, Rusiya Krımı ilhaq etməmiş, ABŞ-ın Bunqazi səfirliyinə hücumu olmamış, İŞİD bu günkü qədər gücə malik olmamış və ABŞ hərbi qüvvələri Əfqanıstandan geri çəkilməmişdi. Bütün bu səbəblərdən, ötən 5

il müddətində beynəlxalq münasibətlərdə yaşanan hadisələr, baş verən dəyişikliklər ABŞ-ın yeni təhlükəsizlik strategiyasını formalaşdırmaq zərurətini ortaya çıxartmışdır [12].

Həm 2002, həm də 2010-cu ildə qüvvəyə minən Milli Təhlükəsizlik Konsepsiyalarından fərqli olaraq, 2015-ci il təhlükəsizlik strategiyasında kiber təhlükəsizlik bölməsinə daha az yer verilmiş və bu haqda fikirlər ümumi sözlərlə ifadə edilmişdir. Xarici siyasət müşahidəçisi David Rotkopf Milli Təhlükəsizlik Konsepsiyasını qiymətləndirərkən sənəddə bir çox ünsürün mövcud olduğunu, lakin əsaslı şəkildə ayırd edilə biləcək strategiyanın olmadığını qeyd etmişdir [18; 66, 2]. Bu bölmədə bildirilirdi: "İnternetin vətəni olan Amerika Birləşmiş Ştatlarının, şəbəkəyə bağlı olan dünyaya liderlik etmək kimi xüsusi məsuliyyəti var. Rifah və təhlükəsizliyi təmin etmək üçün birlikdə çalışmaq, etibarlı internet şəbəkəsi yaratmaq lazımdır. İqtisadiyyatımız, təhlükəsizliyimiz, sağlamlığımız pis niyyətli hökumətlərin, günahkar və fərdi aktorların hədəf götürdüyü şəbəkəyə bağlı infrastruktur ilə əlaqəlidir. Könüllü şəkildə kiber təhlükəsizlik çərçivəsində, ABŞ-ın mühüm infrastrukturlarının təhlükəsizliyini və elastikliyini gücləndirmək üçün federal şəbəkələri zəmanət altına alır, özəl sektor, qeyri-hökumət təşkilatları və digər təşkilatlarla bu sahədə maraqlı olan tərəflərlə birlikdə çalışırıq. Yüksək standartları təmin edən qanunların hazırlanması üçün Konqres ilə əməkdaşlığa davam edəcəyik. Həm ABŞ-ın qanunlarına, həm də beynəlxalq qanunlara uyğun olaraq kiber hücumlara qarşı özümüzü müdafiə edəcəyik. Qanunsuz kiber fəaliyyətin qarşısını almaq, pis niyyətli kiber aktorlarla mübarizə aparmaq üçün maliyyə ayıracağıq. Digər ölkələrə də onlara qarşı yönələn təhdidlərlə güclü mübarizə aparmaq üçün qanunlar yaratmasında yardım əlimizi uzadacağıq. Dövlət, özəl sektor və qeyri-hökumət təşkilatları arasında internetdən istifadəyə tam, rahat şərait yaradacağıq. Biz internetdən istifadə edən hər kəsi informasiya təhlükəsizliyinin təmin olunmasında marağı olan tərəf kimi görürük" [79, 7].

2001-ci il 11 sentyabr terror hadisələri ABŞ-ın yeni informasiya siyasətinin formalaşması üçün dönüş nöqtəsi oldu. Məhz bu hadisələrdən sonra "kiber təhlükəsizlik" 2002-ci il və ondan sonrakı illərdə qəbul olunan Milli Təhlükəsizlik

Strategiyalarının əsas tərkib hissəsinə çevrildi. Müasir dövrdə də davamlı olaraq texnologiya dünyasının dəyişməsi və inkişafı ilə təhdidlərin də sayı artmaqda davam edir. Bu təhdidlərin qarşısını almaq üçün isə qanunvericilikdə daima onlarla mübarizə yolları axtarılır.

FƏSİL 2. ABŞ-ın İNFORMASİYA HÜCUMLARININ ƏSAS HƏDƏFLƏRİ VƏ İSTİQAMƏTLƏRİ

2.1.ABŞ silahlı qüvvələrində şəbəkə strukturu

"Soyuq müharibə" illərinin başa çatması, dünya geosiyasi sistemini və bununla bağlı olan hərbi taktika və strategiyaları, təşkilatları, sistemin ehtiyaclarını kökündən dəyişmişdir. Müdafiəyə ayrılan xərclərin getdikcə azalması, texnologiyaların sürətli inkişafı, sosial-iqtisadi vəziyyətlə yanaşı XXI əsrin əvvəllərində terror hadisələrinin və qarşıdurmaların artması tamamilə yeni hərbi yanaşmalara ehtiyac olduğunu sübut etdi.

1991-ci ildə baş verən I Körfəz müharibəsindən başlayaraq 11 sentyabr terror hadisəsindən sonrakı dövrə qədər hərbi texnologiyaların inkişaf etməsi bu dövrə qədər mövcud olan bütün planların, taktikaların, və strategiyaların da təkamüldən keçməsi zərurətini ortaya çıxarmışdır [20].

Məlum olduğu kimi, informasiya hərbi qüvvələr üçün daima əhəmiyyətli mövzu olmuşdur. Bunun səbəbləri isə aydındır: hərbi qüvvələrin və silahların müştərək nəzarəti sürətli əlaqəni təmin etməlidir. Gərgin vəziyyətlərdə düzgün qərar verə bilmək üçün kifayət qədər informasiya toplamaq lazımdır. Digər sahələrdə də (məsələn iqtisadi) informasiyanın toplanmasına ehtiyac var, lakin bu ehtiyac hərbi qüvvələrdəki qədər böyük əhəmiyyət daşımır. Texniki qurğular yalnız informasiyanın ötürülməsi, saxlanılması və ya toplanması üçün istifadə edilmir, eyni zamanda bu texnologiyalar hərbi əməliyyatlarda da geniş sürətdə tətbiq olunur. Bu sistemlər tərəfindən əldə olunan və işlənən informasiyalar, ordu komandirlərinin düzgün qərar qəbul etməsində vacib rol oynayır [56, 91].

ABŞ-ın Müdafiə Nazirliyinin (Department of Defence) 2015-ci ildə qəbul etdiyi "Kiber Strategiya" adlı sənəddə kiber təhlükəsizliyin təmin olunması üçün beş əsas məqsəd göstərilmişdir:Kiberməkanda əməliyyatların keçirilə bilməsi üçün hərbi qüvvələrin daima hazır vəziyyətdə saxlanılması, qorunması və qabiliyyətlərinin

artırılmasına diqqət yetirilməsi;Ortaq informasiya mühitinin vahid təhlükəsizlik arxitekturasının yaradılması;ABŞ-ın daxili və xarici maraqlarına zidd olan dağıdıcı kiber hücumlardan vacib nəticələrin çıxarılması;Qarşıdurmaların idarə olunması və mövcud olduğu mühitin nizama salına bilməsi üçün kiber planların hazırlanması;Beynəlxalq təhlükəsizliyi təmin etmək üçün dövlətlərarası ittifaqlar və ortaqlıqların yaradılması [74, 5].

"Silahlı qüvvələrin şəbəkə təşkilatları və ya şəbəkə müharibəsi" adlı yeni konsepsiyası 1990-cı illərin sonunda yaranmışdır. Əvvəllər o, müharibə nəzəriyyəsi çərçivəsində informasiya əsrinin yeni təhlükələrini və fürsətlərini proqnozlaşdırmağa yönəlmişdi. Sonralar "şəbəkə müharibəsi" və "hərbi qüvvələrin şəbəkə təşkilatları" terminləri informasiya texnologiyalarının və hərbi işdə təşkilatın şəbəkə prinsiplərinin texniki aspektdən tanıtımı və həyata keçirilməsi üçün hərbi əməliyyatlar zamanı istifadə olunmuşdur. Şəbəkə müharibəsi konsepsiyası informasiya müharibələrinə və informasiya əsrinə həsr olunmuş, təkamül mərhələsidir. Bu sahədə mövcud olan ilk konsepsiya ABŞ-ın silahlı qüvvələrinin inkişafına səbəb olan ilk proqram idi. Belə funksional, inteqrasiyaya tələbatın dərki, silahlı qüvvələrin şəbəkə təşkilatının (Network-centric defence) və ya şəbəkə müharibəsinin (Network-centric warfare) yaranmasına səbəb oldu.

Bu konsepsiyanın müəllifi ABŞ-da Müdafiə Nazirliyinin nəqliyyatın idarəsi üzrə keçmiş direktoru-baş admiral A. Çebrovski və G. Qartska hesab olunur. Silahlı qüvvələrin şəbəkə təşkilatlarının konsepsiyası ilk növbədə informasiya texnologiyalarının və sensor şəbəkəsinin inteqrasiyasına əsaslanır. Bu fəaliyyətə kəşfiyyat peykləri, DRLO təyyarələri-radiolokasiyanın uzaq məsafədən təyin olunması və idarə olunması sistemi və pilotsuz kəşfiyyat təyyarələrinin idarəsi və s. aiddir [30, 86].

A.Çebrovski bildirdir ki,"Şəbəkə müharibəsi konsepsiyası texnologiyalardan bəhs etmir, o hərbi nəzəriyyənin davamıdır" [30, 90]. Çebrovski şəbəkə müharibəsinin digər əsas prinsiplərini müəyyən etmişdir:

1. Geniş informasiya mübadiləsi imkanına sahib olan informasiya paylanması ilə şəbəkə strukturu əsasında dayanıqlı silahlı qüvvələrin yaradılması;

2. Daxil olan informasiyanın keyfiyyət artımı və bütün elementlər arasında informasiya mübadiləsinin yaxşılaşdırılması nəticəsində ümumi hərbi vəziyyət haqqında daha dəqiq təsəvvürün əldə edilməsi.

ABŞ Müdafiə Nazirliyinin rəhbərləri I və II Dünya müharibələri zamanı hava qüvvələrinin müharibənin gedişinə göstərdiyi təsirin, XXI əsrdə internet, qlobal rabitə texnologiyası tərəfindən göstəriləcəyinə inanırdılar. Bu inanclar ordu üçün əhəmiyyətli bir ünsür olan iki fərziyyədə öz əksini tapmışdır: Müharibə vəziyyətində situasiyaların düzgün qiymətləndirilməsi döyüşün təsirinin artmasına səbəb olacaq;Situasiyaların düzgün qiymətləndirilməsi çevik manevrlərə imkan verəcək və qüvvələr daha da hərəkətlənəcək[28, 36].

Bu fərziyyələr ABŞ hərbi qüvvələrinin sənaye dövründən informasiya dövrünə keçidini vurğulayır. Şəbəkə müharibəsinin 4 əsas strateji qanunu müəyyənləşdirilmişdir:Sağlam şəbəkə gücü informasiya mübadiləsini və əməkdaşlığı inkişaf etdirir;Belə mübadilə və əməkdaşlıq, informasiyanın keyfiyyətini və ortaq vəziyyət anlayışlarını inkişaf etdirir;Bundan əlavə, bu yenilik daha çox avtomatik sinxronizasiyaya şərait yaradır;Bu birləşmə fəaliyyətləri əhəmiyyətli dərəcədə sürətləndirir.

Müasir dövrdə Müdafiə Nazirliyində şəbəkə bütün bu dəyişikliklərin ən güclü istiqaməti kimi görünür. ABŞ-ın Müdafiə Nazirliyinin katibi Stiv Boultelin sözlərinə görə silahlı qüvvələrdə təsir edici yeganə amil silah sistemi deyil, eyni zamanda mühüm təsir edici amillərdən biri də informasiya sistemidir [56, 7].

Şəbəkə müharibəsinin tətbiqi Müdafiə Nazirliyinin Güc Transformasiyası Ofisinin (Office of Force Transformation) əsas hədəflərindən biridir. Bu haqda məlumatlar Güc Transformasiyası Ofisinin web saytında da qeyd olunmuşdur [63]. Burada da anlayış "informasiya dövründə inkişaf edən müharibə nəzəriyyəsi" kimi göstərilir. Saytda qeyd olunur ki, şəbəkə müharibəsinin 3 səviyyəsi var: 1) strateji; 2) əməliyyat; 3) taktiki. Bu səviyyələr hərbi əməliyyatlara uyğunlaşdırıla bilər[36, 19-20].

Silahlı qüvvələrdə şəbəkə strukturunun yaradılması bir sıra texnologiyaların inkişafını tələb edir:

1.Şəbəkə arxitekturası.Silahlı qüvvələrin şəbəkəsinin ümumi effektivliyi ilk növbədə istifadə olunan informasiya-kommunikasiya avadanlığının uyğunluğundan asılıdır. Bu səbəbdən, informasiyanın qəbulunun və saxlanılmasının vahid bir standartda olması əsas prioritetdir. Bunsuz şəbəkə prinsiplərinin reallaşdırılması mümkün olmur. Silahlı qüvvələrdə bir-birinə uyğun olmayan və ya az uyğun olan müxtəlif sistemlərdən (radioəlaqə, kosmik sistem və s.) istifadə olunduğundan problemin həlli daha da çətinləşir. Beləliklə, informasiyanın qəbul olunması və saxlanılması vahid rəqəmsal standart və rəqəmsal informasiya proqramı üçün bir protokol tələb olunur.

Müasir dövrdə daha çox tanınmış Amerikan standart internet protokolu proqram paketi olan NİPRNet (Non-classified Internet Protocol (IP) Router Network-gizli olmayan məlumatlar) və SİPRNet (Secret Internet Protocol Router Network-gizli olan məlumatlar) hərbi protokollardır. Onlar arasındakı fərq ondan ibarətdir ki, SİPRNet kənar şəxslərin istifadəsindən izolyasiya olunmuş internet şəbəkəsindən, NİPRNet isə açıq internet kanallarından istifadə edir. Yaxın zamanlara qədər hərbçilər gizli məlumatların göndərilməsi üçün xüsusi şifrələmə texnologiyaları vasitəsi ilə açıq kanallardan istifadə edirdilər. Ekspertlərin fikrincə, yaxın zamanda hərbçilər tamamən SİPRNetdən yararlanacaqlar [30, 94].

2.Peyklər.Peyklərin istifadəsi uzaq bölgələrdə əlaqənin yaradılması naviqasiya, kartoqrafik və meteoroloji informasiyanın əldə olunması və həmçinin raketdən müdafiə sisteminin əvvəlcədən xəbərdar olmasında əvəzolunmaz rol oynayır (ABŞ-da raketdən müdafiə sistemi NMD-National Missle Defence adlanır). ABŞ-ın orbital qrupunda 28 CPS naviqasiya sistemi peyki, 6 orbital kəşfiyyat sistemi kompleksi, 1 milli raketdən müdafiə sistemi-əvvəlcədən xəbərdarlıq peyki, 2 kəşfiyyat obyekti və 3 radioqəbuledici peyki var. Lakin bütün bu təchizatlara baxmayaraq, ABŞ-ın silahlı qüvvələri və koalisiya üzvlərinin "İraqa azadlıq" hərəkatı zamanı informasiya sisteminin idarə olunmasında istifadə olunan 84% radiotezlikləri kommersial xarakter daşıyırdı [30, 94].

3. İş radiotezliyi.Məlumatların rəqəmsal standartlara uyğunlaşdırılması silahlı qüvvələrin transformasiyasının demək olar ki, bütün proqramlarını əhatə edir.

Rəqəmsal texnologiya tezliklərin iş diapazonunu daha effektiv istifadə etməyə icazə verir ki, bu da analoqu olan bir əlaqədir. Belə ki, bu zaman bir diapazonda kanalların kəmiyyəti 6-10 dəfə artır [30, 95].

4.Pilotsuz aparatlar.Əsasən kəşfiyyat xarakteri daşıyan pilotsuz aparatlara uçan, yerüstü və sualtı aparatlar aid edilir ki, bunlara son zamanlar zərbə yetirmək funksiyasının əlavə edilməsi də düşünülür. Bundan əlavə, pilotsuz aparatlar şəbəkə əməliyyatları zamanı informasiya transformasiyası qovşağı kimi istifadə olunur. Pilotsuz aparatların istifadə perspektivi əlaqə tezliyi diapazonunun genişlənməsinə səbəb olur [30, 95].

5.Kompüter prosessorları.Klassik qanuna çevrilən hər 1,5 ildən bir kompüter prosessorlarının 2 dəfə artırılması Q.Murom tərəfindən formalaşdırılmış və ABŞ-ın kompüter texnologiyası siyasətinin əsasını təşkil edir. Bu səbəbdən hərbi qüvvələrin şəbəkə konsepsiyasının reallaşması ilə əlaqədar proyektlərin əsas hissəsi kompüter sisteminin daimi təkamülü sayılır [30, 95].

6.Nanotexnologiya.Müasir dövrdə ABŞ silahlı qüvvələrində gəmi turbinlərinin və raket yanacaqlarının keyfiyyətini artırmaq üçün nanotexnologiyalardan istifadə olunur. Bu texnologiyadan istifadə edərək bir çox sistemləri radikal şəkildə dəyişməyin mümkün olacağı düşünülür. Əsasən individual müdafiə və daha çox yüklənə bilən elektrik stansiyalarının yaradılmasında istifadə olunacaq yüksək səviyyədə sərt və elastik, yüngül materialların hazırlanması gözlənilir. Həmçinin rəqibin hədəfini yüksək dəqiqliklə tapan, müəyyənləşdirən, müşayət edən və informasiya şəbəkəsinə qoşula bilən, miniatür sensorların hazırlanması perspektivləri vardır. Bu məsələ ilə bağlı 2003-cü ildə Massaçusets Texnologiya Universitetinin nəzdində Hərbi Nanotexnologiyalar İnstitutu (İnstitute for Soldier Nanotechnologies) açılmışdır. Bu haqda qərar 2002-ci ildə qəbul edilmiş, kimyəvi və bioloji silahlar üçün daşına bilən detektorların müasir piyada sursatından 15 kq daha yüngül olan sensorlu elastik ekzoskletlərin hazırlanması üçün quru qüvvələrindən 50 milyon qrant ayrılmışdır [30, 96].

7.Proqram təminatı.Proqram təminatı bütün informasiya sistemlərinin ən vacib komponentidir. ABŞ-ın silahlı qüvvələri audit idarəetməsini, proqram təminatının

kommersial layihələrinin əsas baza komponenti kimi istifadə olunmasını təklif edir. Bu təkliflərlə əlaqədar olaraq Müdafiə Nazirliyi (Department of Defence) proqram təminatının hazırlanması üçün satış firmaları ilə bəzən isə afşor firmalarla subkontraktlar imzalayır. Pentaqonun sifarişi ilə hazırlanmış proqram təminatının özündə informasiyanın icazəsiz istifadə olunmasına imkan verən kodlar və fraqmentlər və ya komputer sistemini sıradan çıxardacaq funksiyalara sahib olmaq təhlükəsi mövcuddur. ABŞ silahlı qüvvələrinin informasiya təhlükəsizliyi idarə edilməsi üzrə direktoru R.Linçin fikrincə, bu təhlükələr bir qədər şişirdilib. Belə ki, hərbçilərin informasiya sisteminin təhlükəsizliyini artırmaq üçün yetərincə effektiv metodlar vardır. Bununla belə, bəzi ekspertlər bu metodlara şübhə ilə yanaşırlar, çünki virus proqramlarını onlar işə düşmədən daha əvvəl müəyyən etmək demək olar ki, mümkün deyil [30,97].

Bu prinsiplərin reallaşdırılması və perspektivli texnologiyalar əsasında vahid informasiya arxitekturasının yaradılması aşağıdakı xüsusiyyətlərin effektivliyini artırmağa icazə verir:Hava-quru-dəniz əməliyyatları kompleksində qarşılıqlı əməkdaşlığın artırılması;Şəbəkə hərbi qüvvələrinin təchizatı sadələşdirən və xərcini aşağı salan daha kompakt mobil bölmələrdən ibarət olması;Hərbi əməliyyatların aparılması üçün yeni taktikaların yaradılması;Çətin hərbi şəraitdə qərarların qəbulunu asanlaşdıran sadə idarəetmə sisteminin yaradılması;Rəqibin fəaliyyətinə daha qısa müddətdə reaksiya verilməsi (hədəfin təyin olunmasından, qərarın qəbuluna və onun məhv edilməsinə qədər).

Yeni taktikanın bəzi xüsusiyyətləri artıq yoxlanışdan keçirilib. Məsələn, 2003-cü ildə ABŞ-ın İraqdakı əməliyyatları zamanı maddi-texniki dəstək sisteminin təmamilə yerləşdirilməsini gözləmədən hərbi qüvvələrin irəli getməsinə imkan verən "sürü taktikası" tətbiq olunmuşdur [32]. Yaradılmış informasiya şəbəkəsi rəqibin ərazisində müstəqil kompakt bölmələrin sürətlə yerləşdirilməsinə icazə verən informasiya mübadiləsinə dəstək olur. Hər bir bölmə döyüş meydanının tam təsvirini əhatə edirdi: digər bölmələrin harada yerləşməsi və onların rəqib haqqında əldə etdikləri məlumatlar.

Komandir rəqibin daha çox qarşı durduğu ərazilərə əlavə qüvvələr göndərmək haqqına sahib idi. "Savaş sürüləri" taktikasının tərəfdarlarının fikrincə onun inkişafı silahlı qüvvələrin və silahların kəmiyyətini azaltmağa icazə verəcək. Bu isə öz növbəsində hərbi sahəyə xərclərin azaldılması deməkdir[29, 91].

Şəbəkə müharibələri silahlı qüvvələrin informasiya dövrünə cavabıdır [40, 3]. Şəbəkə müharibələrinin gətirdiyi yenilik isə informasiya texnologiyalarının kosmos sistemləri ilə birgə istifdə olunmasıdır [44, 143].

"Soyuq müharibə"nin başa çatması ilə, yeni geosiyasi sistem formalaşdı, hərbi taktika və strategiyalarda köklü dəyişikliklər baş verdi. Belə ki, müdafiəyə ayrılan xərclərin azalması, texnologiyaların sürətli inkişafı XXI əsrin əvvəllərində terror hadisələrinin və qarşıdurmaların artması sosial-iqtisadi vəziyyətlə yanaşı yeni hərbi yanaşmalara ehtiyac olduğunu sübut etdi. Bu dövrdə ABŞ-da "Silahlı qüvvələrin şəbəkə strukturu və ya şəbəkə müharibəsi" adlı yeni konsepsiya yarandı. ABŞ Silahlı qüvvələrində şəbəkə strukturunun yaradılması bir sıra texnologiyaların inkişafını tələb edir. Bu texnologiyalara peyklər, pilotsuz aparatlar, nanotexnologiyalar, kompüter prosessorları və b. daxildir. Texnologiyaların sürətli inkişafı mütəmadi olaraq ABŞ silahlı qüvvələrində də şəbəkə struturunun yenilənməsinə, yeni plan, taktika və strategiyaların hazırlanmasına gətirib çıxarır.

2.2.İnformasiya müharibələrində ABŞ-ın media korporasiyalarının iştirakı

Sosial həyatda xüsusi yeri olan medianın fərd, cəmiyyət, mədəniyyət və nəhayət,siyasi sahə ilə olan əlaqəsi danılmazdır. Beynəlxalq münasibətlər çərçivəsində isə "media" anlayışı, qloballaşmanın və texnologiyanın təsirlərini də özündə cəmləşdirmişdir. Bu münasibətlərdə dövlətlərin xarici siyasətini şərh etməyə yönəlmiş müzakirələrdə ənənəvi yanaşmalardan kənara çıxılmış, xarici siyasət ilə əlaqəsi olan hər cür anlayışlar və faktlar (şəxsiyyət, ətraf və s.) beynəlxalq münasibətlərin müzakirə mövzusuna çevrilmişdir.

İnformasiya müharibələrində medianın rolu danılmazdır. Qədim dövrdən müasir dövrə qədər olan zaman çərçivəsində informasiya müharibələrini medianın fəaliyyəti olmadan təsəvvür etmək demək olar ki, mümkün deyil. ABŞ-ın media korporasiyaları müasir dövrdə baş verən informasiya müharibələrində öz əhəmiyyətinə, əhatə dairəsinə, təsir imkanlarına görə bir çox ölkələrin media korporasiyalarından fərqlənir.

ABŞ mediası, televiziya, radio, kino, qəzet, jurnal, internetə əsaslanan veb saytlarla birgə bir çox media növündən ibarətdir. Bu gün ABŞ-da media, "Dördüncü Hakimiyyət" kimi tanınır. Mətbuat və ya "Dördüncü hakimiyyət" ABŞ demokratiyasının qoruyucusu kimi olduqca əhəmiyyətli rola malikdir. Bu rol Konqresin mətbuat azadlığını məhdudlaşdıran hər hansı bir qanun çıxarmayacağını nəzərdə tutan və 1789-cu ildə qəbul edilən ABŞ Konstitusiyasının birinci dəyişikliyində əksini tapır[77].

Birinci dəyişiklikdə qeyd olunur ki, Konqres hər hansı bir din müəssisəsinə hörmətlə yanaşmalı və dini ibadət sərbəstliyini yasaqlamağa yönəlmiş, həmçinin söz və mətbuat azadlığını, xalqın dinc toplaşmaq və şikayətlərinin aradan qaldırılması üçün hökuməti sorğu etmək hüququnu məhdudlaşdıran heç bir qanun verməyəcək [35].

ABŞ mediası, 1690-cı ildə Massaçusetsdə nəşr olunan və ilk qəzet olan "Boston" qəzetinin yayımlandığı gündən bu günə qədər uzun yol qət etmişdir. 50 il ərzində jurnallar, qəzetlər ABŞ-ın digər şəhərlərində də yayılmağa başlamışdır. XX əsrin əvvəllərində ticarət radiolarının yaranması ilə əlaqədar olaraq, ABŞ mediası artıq yalnız ölkə daxilində deyil, ölkədən xaricdə də öz yayımlarını etmək imkanı qazandı. İnformasiya müharibələrində ABŞ-ın radio yayım sistemlərinin rolu çox böyükdür. Bu radiolardan hal-hazırda bütün dünyada məşhur olan "Amerikanın səsi" (Voice of America) radiosunu misal göstərmək olar. "Amerikanın səsi" radiosuABŞ hökumətinin xarici auditoriya üçün nəzərdə tutulmuş xəbər yayımlama təşkilatıdır. Bu radionun əsas məqsədi "Amerika və dünya haqqında xarici auditoriyaya multimedia formatında dəqiq, obyektiv və balanslı informasiya verməklə azadlığı, müstəqilliyi və demokratiyanı təşviq etməkdir". İkinci dünya müharibəsi illərindən,

yəni 1942-ci ildən fəaliyyət göstərən "Amerikanın səsi" radiousu hal-hazırda internetdə, televiziya və radioda 43 dildə verilişlər yayımlayır [71].

Medianın daha güclü növlərindən biri olan televiziyalar İkinci Dünya Müharibəsindən sonra meydana gəldi. Peyk texnologiyası isə ABŞ-dakı TV şəbəkələrinin, xüsusilə də kabel şəbəkələrinin dünyanın hər yerində yayılmasına şərait yaratdı. Rəqəmsal texnologiyaların inkişafı, kompüter, telefon və kabel televiziyasının hərəkətə keçməsi ilə XX əsrin sonu - XXI əsrin əvvəllərində ABŞ mediası daha da güclənərək öz fəaliyyətini genişləndirdi.

SSRİ dövründə hökumət mediaya nəzarət edirdi. Bolşevik komissarlarının əvvəlcədən təsdiqi olmadan bir kəlmə belə nəşr oluna bilməzdi. Bu gün ABŞ-da da vəziyyət buna bənzəyir. Hazırda Birləşmiş Ştatlarda mövcud olan bir çox zəngin ailələr ya böyük media qurumlarının sahibidirlər ya da onlar üzərində güclü nəzarətə malikdirlər.

Böyük media kanallarının hər biri üzərində demək olar ki, güclü nəzarət mövcuddur. Hətta "New Orleans Times" kimi "regional nəhənglər"ə belə nəzarət olunur. "ABC", "CBS", "CNN", "Time", "Newsweek", "US News & World Report", "New York Times", "Washington Post", "Los Angeles Times", "Chicago Tribune", "Miami Heralt", "San Diego" və s. - siyahı beləcə uzanıb gedir - kimi media qurumları hamısı nəzarət olunanlar siyahısına daxildir. Bu media kompaniyalarının ABŞ-da və dünyanın dörd bir yanında gündəlik, həftəlik qəzetlər, jurnallar, radio və televiziya verilişləri və s. hamısının üzərində xüsusi diqqət vardır.

Orta hesabla hər 10 amerikalıdan biri, Rokfeller, Rotşild, Bronfman, Nyuhaus, Murdoç və Redstoun kimi zəngin ailələrin həm ABŞ, həm də dünya mediasına böyük investisiya yatırdığını düşünürlər. Bu zəngin ailələr və şirkətlər "media ustaları" adlandırılır. Onlar haqqında aşağıdakı fikirlər mövcuddur:

- media ustaları hansı mövzunun müzakirə olunub-olunmayacağına qərar verir;
- media ustaları hansı müharibələrin "yaxşı müharibə", hansının isə "pis müharibə" olmasına qərar verirlər;
- media ustaları kimin "qəhrəman", kimin isə "pis" olduğuna qərar verirlər.

1983-cü ildə 50 böyük şirkət ABŞ xəbər mediasının böyük əksəriyyətini idarə edirdi [85].

1989-cu ildə qlobal media monopoliyasında 11 ən böyük media təşkilatı digərlərindən fərqlənirdi. 2007-ci ilə əsasən bu rəqəm 9-a, 2012-ci ilin statistikasına əsasən isə bu şirkətlərin sayı 6-ya enmişdir.

"Associated Press" və ya qısaca olaraq "AP" ABŞ-ın xəbər agentliyidir və dünyanın ən qədim, ən böyük media təşilatıdır. ABŞ-ın xaricindəki bir çox qəzet və nəşriyyat orqanları "AP"ın üzvüdür. "AP" minlərlə qəzet, radio və televiziya stansiyalarını informasiya ilə təmin edir.

Əsas xəbər stansiyalarının hər birində dünyanın dörd tərəfindən agentlər vasitəsilə video, şəkil, xəbər göndərən kompüterlər mövcuddur. Böyük xəbər agentlikləri video və fotoşəkilləri aldıqdan sonra, xəbərləri lazım olan istiqamətə yönləndirirlər. İraq müharibəsi zamanı NBC-nin (Nation Broadcasting Corporation) xəbər tədqiqatçıları müharibənin yaxşı getdiyini göstərmək üçün əsgərlərin yol gedərkən gülən yerdə şəkillərini yayımlamışdılar.

AP-ın xəbərləri 2005-ci ildən etibarən 1700 qəzet, 5000 televiziya və radio yayım orqanı tərəfindən istifadə edilir. Foto kitabxanasına 10 milyondan artıq şəkil daxildir. AP 121 ölkədə xidmət göstərən və 243 büroya malik olan ən böyük xəbər agentliklərindən biridir[85].

İsrail hərbi qüvvələri 2004-cü ilin 17 oktyabrında Fələstinin ən kasıb, əhalisinin sayına görə isə sıx ərazilərindən biri olan Balatanı işğal etdi. Şahidlərin ifadəsinə görə, fələstinlilər heç bir müqavimət göstərməmişdilər, "qarşıdurma", hətta daş atmaq belə yox idi. Ordu bu ərazidən çıxarkən bir İsrail əsgəri zirehli maşından silah çıxararaq qarşıda olan 12 yaşlı Muhammməd El Dorrayı hədəfə alır və atəş açaraq onun ölümünə səbəb olur. AP-nin bir kameramanı hər hadisəni filmə çəkmişdi. Müharibədə çəkilən bu görüntülər sənədli dəlil olduğu üçün son dərəcə qiymətli bir video çarx idi. GörüntüAP-nin nəzarət bürosuna göndərilmişdir. Bu büro İsraildə yerləşirdi və təbii olaraq, video yayımlanmadı [85].

Son illərdə, beynəlxalq münasibətlərin müşahidəçiləri, medianın ABŞ diplomatiyasının və xarici siyasətinin davranışlarına təsirinin artdığına dair

informasiyalar verirlər. “CNN effekti” (başqa adla “CNN əyrisi”, “CNN faktoru”) adlandırılan bu təsir çox böyük effektə malikdir. Bunun üçün iki əsas səbəbi göstərmək olar: Soyuq müharibənin başa çatması; Texnologiyanın yüksək inkişafı. İnformasiya texnologiyalarının sürətli inkişafı dünyanın hər yerindən canlı yayım etmək imkanı yaradır [53, 1].

“CNN” (Cable News Network), “Ted Turner” tərəfindən 1980-ci ildə iyunun 1-də Atlantada yaradılmış xəbər kanalıdır. Kanal yarandığı gündən bu günə qədər ABŞ-da 24 saat xəbər yayımlayan ilk kanaldır. CNN mütəmadi olaraq dünyanın 212 ölkəsində 1,5 milyarddan çox insan tərəfindən izlənir. Kanal müxtəlif dillərdə yayımlanır. CNN 2 radiosu, 12 vebsaytı və bütün dünyaya yayılmış xəbər qrupu ilə ən məşhur xəbər qaynaqlarından biri hesab olunur [53, 3].

1991-ci ildə Birinci Körfəz müharibəsi zamanı Bağdaddan döyüşü canlı olaraq yayımlaması CNN-i bütün dünyada məşhurlaşdırdı. CNN-in yayımları ilə televiziya xəbərçiliyində yeni dövr başladı. 2010-cu ilin avqust ayına olan məlumata əsasən, CNN ABŞ-da 150 milyon insan tərəfindən izlənir.

“CNN effekti”, siyasi elm və media araşdırmalarında, "News Network" və CNN kimi tanınan məşhur, 24 saat fasiləsiz canlı yayım həyata keçirən Soyuq müharibənin son dövrlərində, dövlətin xarici siyasətinin gedişinə əhəmiyyətli təsiri olduğunu vurğulayan nəzəriyyədir. Soyuq müharibədən sonrakı dövrdə də buna bənzər şəkildə CNN-in fəaliyyəti davam edir. “Dördüncü hakimiyyət” adlandırılan və sərbəst şəkildə fəaliyyət göstərən media demokratik dövlətlərdə hər zaman böyük təsirə malik olsa da, “CNN effekti”nin tərəfdarları, yeni qlobal medianın əhatəsini, dərinliyini və surətini tarixən əvvəlkindən keyfiyyət baxımından fərqli olduğunu yeni növ effektlərinin ortaya çıxdığını bildirirlər[53, 2].

“CNN effekti” nəzəriyyəsi qlobal televiziya kanalının, bir ölkənin müdafiəsi və xarici siyasətinin yaradılmasında birbaşa, hətta baş faktor olmasını göstərən nəzəriyyədir. Bu nəzəriyyə CNN-in böyük həcmdə siyasi qurumların fəaliyyətində, qlobal əlaqələrdə, xüsusilə də Soyuq müharibədən sonraki dövrdə müəyyən beynəlxalq qarşıdurmalarda oynadığı rollara bağlı düşüncələrləəlaqəlidir. CNN Çin hökumətinin Pekinin “Tiananmen” meydanındakı şagirdlərin etiraz

nümayişlərini şiddətlə yatırması zamanı, İraqın Küveyti işğalının ardından sonra baş verən 1990-1991 Körfəz Böhranının, 1991-ci ilin avqustunda Rusiyadakı çevriliş cəhdinin və Şimali İraq, Somali, Ruanda, Bosniya və Kosovada baş verən daxili münaqişələrin yayımını təşkil etmişdir [36, 10].

CNN effekti ilə əlaqədar elmi araşdırmalar olduqca qarışıq və ziddiyyətlidir. 1994-cü ildə Kohen, 1996-ci ildə isə Bernard Şou bu qlobal televiziya kanalının həyata keçirtdiyi yayım nəticəsində, 1991-ci ildə kürdləri xilas etmək üçün Şimali İraqa və 1992-ci ildə Somalidə daxili münaqişələri yatırmaq üçün ABŞ siyasətçilərini bu ölkələrə müdaxilə etməyə məcbur etdiyini iddia edirdilər. Digər araşdırmalarda isə bu qlobal televiziyanın siyasətçilərin qərarlarına nəzarət edib etmədiyi, onları müdaxiləyə məcbur edib etmədiyi, ya da yalnız müəyyən bir təsirə saldığı haqqında düşüncələr öz əksini tapmışdır. Məsələn, Goving 1994-cü ildə CNN yayınlarının böhranlara gətirdiyini və xalqın hislərini hərəkətə keçirdiyini qeyd etmişdir[36, 11].

"CNN effekti"nin xarici siyasətə təsirini əvvəlki medianın təsirlərindən ayıran əsas səbəb onun qloballaşması, real vaxt keyfiyyətinin yüksək olmasıdır. Ancaq tam şəkildə bu təsirlərin nədən ibarət olduğu, hansı şəraitdə ortaya çıxdığı və hətta var olub-olmadığı ən çox müzakirə olunan mövzulardandır.

Beynəlxalq arenada baş verən hadisələr media məsələlərinə diqqətlə yanaşmağı tələb edir. Marqaret Belknapa görə: "CNN effekti real vaxtda xəbərlərin ortaya çıxması, ictimaiyyətin şüurlu formada məlumatlandırılması, strateji qərarların və hərbi əməliyyatların araşdırılmasına gətirib çıxardı"[36, 3].

Birləşmiş Ştatlardakı çap və elektron mühit geniş xəbər və əyləncə variantları təqdim edir və Amerika cəmiyyətində əhəmiyyətli faktordur. "Mediamark Research"in həyata keçirdiyi anket sorğusuna görə, amerikalıların 98%-də ən azı bir televizor var. Əhalinin 82%-i "prime time", 71%-i isə kabel proqramlaşdırmasını orta hesabla, bir həftə izləyir. Amerikalıların 84%-i nizamlı olaraq radio dinləyir, 79% isə qəzet oxucusu mövcuddur. ABŞ əhalisinin 45%-i internet istifadəçisidir. Müəyyən demoqrafik qruplarla birgə bu göstərici 70%-ə çatır[77].

Müasir dövrdə informasiya müharibələrində ABŞ-ın yazılı mətbuat orqanlarının da rolu kifayət qədər böyükdür. Bu gün dünyada məşhur olan "The New

York Times", "Washington Post", "The Wall Street Journal", "USA Today", "Time" kimi qəzet və jurnallar milyonlarla insan tərəfindən oxunur.

"The New York Times" qəzeti 1851-ci il, sentyabrın 18-də fəaliyyətə başlamışdır. Nyu York şəhərində nəşr olunan gündəlik qəzetlərdən biridir. Qəzetin sahibi "The New York Times Company"-dir. Bu qəzet Barak Obama və Demokratlar partiyasının dəstəkçisi kimi tanınır.

"Vaşinqton Post" ("The Washington Post") qəzeti ABŞ-ın paytaxtı Vaşinqton şəhərində dərc olunur. Qəzet 1877-ci ildə Demokratlar Partiyasının üzvü Stilson Xatçins tərəfindən təsis edilib. Qəzetin ilk sayı 1877-ci il, dekabrın 6-da 10 min tirajla, 4 səhifə həcmində işıq üzü görüb. 2005-ci ilin hesablamalarına görə, "Vaşinqton Post" ABŞ-ın ən yüksək tirajlı beşinci qəzeti hesab olunur. Həmin il oxucularının sayı orta hesabla, iş günləri 715 min 181 nəfərə, bazar günləri isə 983 min 243 nəfərə çatıb. Şəxsi mülk kimi təsisçinin ailəsinə məxsus olan "Vaşinqton Post" digər media və qeyri-media strukturlarına malik eyni adlı şirkətin tərkib hissələrindən biridir. "Vaşinqton Post"un ABŞ-dan xaricdə – Bağdad, Pekin, Berlin, Boqota, İslamabad, Yerusəlim, Kabil, London, Mexiko, Moskva, Dehli, Paris və Tokioda büroları fəaliyyət göstərir.Qəzet beynəlxalq sahədə olan mövzulara geniş yer ayırması ilə fərqlənir [7].

Qəzetin tarixində ən çox iz qoyan hadisələrdən biri məşhur "Uotorgeyt" qalmaqalıdır. 1974-cü ildə "Vaşinqton Post" qəzeti ABŞ prezidenti Riçard Niksonun siyasi rəqiblərinin gizli dinlənməsində iştirakını üzə çıxarmış və "Uotorgeyt" qalmaqalı kimi tarixə düşən bu hadisə dövlət başçısının istefası ilə nəticələnmişdir [7].

İnternetin vətəni olan ABŞ öz vebsaytları ilə bütün dünyada məşhurdur. İnformasiya müharibələrində vebsaytların rolunu xüsusilə qeyd etmək lazımdır. Axtarış sahəsində Google saytı, video paylaşımı sahəsində-Youtube, Vikipedia ensiklopedia saytı, xəbərlər sahəsində Google News, elektron ticarət, onlayn auksion və alışveriş sahəsində-Amazon, eBay, proqram təminatı sahəsində- Microsoft, Windows live, media və əyləncə sahəsində-Yahoo!, Reddit, Wordpress.com kimi

vebsaytlar qlobal vebsaytlara çevrilmişdir. Facebook, Twitter, İnstagram kimi məşhur sosial şəbəkələr ABŞ-ın informasiya müharibələrində əsas güc mənbələrindəndir.

Medianın başqa bir növü də seçmə mediadır. Bəzən bu növ mediaya "gündəm təyinedici media" da deyilir. Bunun səbəbi, böyük qaynaqlara sahib olmaqla, başqa media orqanları arasında gördüyü işlə fərqlənən media təşkilatlarının mövcud olmasıdır. New York Times, CBS bu növ təşkilatlara aiddir. Bu media orqanları kifayət qədər yüksək qazanc əldə edən şirkətlərdir. Üstəlik əksər media şirkətləri General Motors, Washingtonhouse və s. kimi ya böyük şirkətlərlə bağlıdır ya da birbaşa onların mülkiyyətindədir. Onların oxucularının, tamaşaçılarının əksəriyyəti imtiyazlı insanlardır. Nyu York Times-ı oxuyan insanlar zəngin və ya bəzən "siyasi sinif" adlandırılan sinfin üzvləridir. Bu təbəqələr davamlı şəkildə siyasi sistemin içində iştirak edirlər. Bunlar şirkət rəhbərləri, universitet professorları və ya jurnalistlər ola bilər [24].

Məlumdur ki, fiziki müharibə aparmaq üçün ilk növbədə informasiya müharibəsi aparılmalıdır. Müharibələrin tərkib hissəsi olan informasiya müharibələrində ABŞ öz fəallığı ilə xüsusilə fərqlənir. I və II Körfəz müharibələri zamanı ABŞ mətbuatı geniş fəaliyyət göstərmişdir.

Səddam Hüseynin dövründə İraqın Küveyti işğal etməsi, Sovet Rusiyasının lider olduğu Varşava Paktının çökməsi ilə birlikdə "Yeni Dünya Nizamı" yarandı. Bu çərçivədə ABŞ və müttəfiqləri 1991-ci ildə hava hücumları ilə İraqa müharibə elan etdilər. İlk vaxtlarda yayımlanan məlumatlarda müharibənin qaçınılmaz olduğu fikri hakim idi. Aparılan bir araşdırmada, müharibədən əvvəlki 6 ay ərzində, ümumi 48 saatlıq xəbər müddətində müharibənin lazım olmadığı, yalnız 29 dəqiqəlik bir zaman müddətində müharibənin lazım olduğu fikri yer almışdır [61, 14]. Bu xəbərlərdə S.Hüseyndən canavar, şeytan, zalım, barbar kimi bəhs edilmişdir.

Digər bir araşdırmada, müharibədən üç gün əvvəl tamamlanan anketdə Amerika xalqı arasında hərbi müdaxilə ilə əlaqədar olaraq fikir ayrılıqları mövcud idi. The New York Times-CBS News tərəfindən həyata keçirilən anket sorğusunda xalqın 47%-i hərbi müdaxilənin tərəfdarı olduğu halda, 46%-i embarqo və iqtisadi sanksiyaların işə yarayıb-yaramayacağını görmək üçün gözləmək lazım olduğunu

ifadə etmişdir. Müharibə başladıqdan sonra təkrarlanan anket nəticələrinə görə isə 76% müdaxilənin haqlı olduğu fikrini müdafiə etmiş, yalnız 19% iqtisadi sanksiyalar üçün zaman ayrılması lazım olduğunu ifadə etmişdir. Eyni araşdırmada, prezident Buşa verilən dəstəyin də 67%-dən 84%-ə çatdığı aydın olmuşdur [17, 69].

ABŞ-dan Körfəz müharibəsinə göndərilən jurnalistlərin çoxu Buş administrasiyasına daxil olan jurnalistlər idi. Digər jurnalistlər üçün isə Pentaqon anket sorğusu hazırlamış, verdikləri cavablara əsasən jurnalistlər müharibə bölgəsinə göndərilmişdir. Birinci Körfəz müharibəsində ümumilikdə 1600 jurnalist iştirak etmişdir[21, 317].

"Time" müxbiri Con Staks I Körfəz müharibəsini XX əsrin qapıları möhkəm şəkildə bağlı olan müharibəsi kimi xarakterizə etmişdir [13, 72].

Müharibəni izləyən jurnalistlərə Pentaqon tərəfindən 2 səhifəlik qadağan siyahısı verilmişdir. Bu siyahıya jurnalistlərin gecələr işıq istifadə etməsinin məhdudlaşdırılması, ölü və yaralı adlarının, hərbi bazaların yerləşməsinə və nəqlinə aid, döyüş təyyarələri ilə əlaqədar hərbi hərəkatın və hərəkatda vəzifə başında olan heyətin təhlükəsizliyini risk altına ata biləcək, reallaşdırılacaq hərbi hücumlarla bağlı, müttəfiqlərin müharibədə məğlubiyyəti, ya da hərbi vəzifələrlə bağlı ABŞ qoşunları əleyhinə istifadə edilə biləcək informasiya sızmasının qarşısının alınması daxil idi [21, 319].

Xəbərlər, çəkilən fotoşəkillər və videolar Pentaqon rəsmiləri tərəfindən yoxlanılmış, onlara senzura tətbiq olunmuşdur. Təsdiqlənən xəbərlər jurnalistlərin istifadəsinə verilmişdir. Beləcə, yalnız Pentaqon rəsmiləri tərəfindən təsdiqlənən xəbərlər bütün dünya tərəfindən təqib oluna bilmişdir. Bununla əlaqədar olaraq, müharibə ictimaiyyətə qansız, təmiz müharibə kimi əks olunmuşdur. Halbuki tarixin ilk müasir informasiya texnologiyası müharibəsi kimi tanınan Birinci Körfəz müharibəsində təkcə Bağdada tonlarla bomba atılmış, müharibədə təxminən 150 min İraq əsgəri həlak olmuş, 200 min İraq əsgəri yaralanmış, İraq sanki yerlə-yeksan olmuşdur. Müharibədə müasir informasiya texnologiyaları sayəsində vətəndaşların deyil, bazaların və hərbi obyektlərin hədəfə alındığı, bu səbəbdən də vətəndaşların ölmədiyi düşüncəsi formalaşmışdır. Beləliklə, müharibədə İraqın üzərinə atəş açan

təyyarələrin kameralarından alınan görüntülər bütün dünya ictimaiyyətinə video və ya kompüter oyunu kimi izlədilmişdir [11, 139].

Birinci Körfəz müharibəsi, Bağdadda qalmasına icazə verilən yeganə mətbuat orqanı CNN vasitəsilə bütün dünyada izlənilmişdir. İnformasiya texnologiyalarındakı yeniliklər bu dəfə müharibənin canlı yayından izlənilməsinə imkan versə də, CNN müxbirləri Piter Arneft, Con Holiman və Bernard Şeyv Bağdadda hadisələri təxminən 5 km uzaqdan, Əl-Rəşid otelindən təqib edə bilmişdilər.

Birinci Körfəz müharibəsində 24 saat canlı yayın həyata keçirən CNN rəqibləri ABC, CBS və NBC-dən bir addım önə çıxaraq xəbərçilik anlayışına yeni forma vermişdir. Müharibədə istifadə edilən yeni kommunikasiya texnologiyalarına daşına bilən kompüterlər, rəqəmsal şəkil ötürülməsini təmin edən aparatlar, hərəkətsiz videokameralar, qaranlıqda görmək üçün istifadə olunan cihazlar, fakslar, peyk əlaqəli daşınan telefonlar və s. daxildir.

Birinci Körfəz müharibəsində sistemdən məmnun qalmayan mətbuat orqanları, Pentaqondan qarşıdurmaları və müharibələri izləyərkən daha azad şəkildə fəaliyyət göstərmək üçün bir sıra dəyişikiliklər olunmasını tələb etmişdilər. Bunun nəticəsində, 1992-ci il martın 11-də Pentaqon ilə ABŞ mətbuatı arasında 9 maddədən ibarət protokol imzalanmışdır[15, 81].

Bu protokol bir çox istiqamətdən tənqid olunmuşdur. Xüsusilə, 4-cü maddədə vurğulanırdı ki, müharibə gedən bölgədə qaydalara riayət etməyən jurnalistlər döyüş bölgəsindən qovulacaq, bölgədən xəbər yayımlanması qadağan ediləcək. 6-cı maddədə isə qeyd olunurdu ki, hərbi səlahiyyətlilər və əsgərlər milli təhlükəsizlik maraqlarına aid olan informasiyaların sızdırılmaması məqsədi ilə mətbuat nümayəndələrinin işinə müdaxilə edə bilərlər. Bu iki maddə xüsusilə narazılıqlara səbəb olmuşdur.

Media təşkilatları, müharibə bölgələrində səlahiyyətlərini icra edəcək jurnalistlərin göndərəcəkləri fotoşəkillərin və xəbərlərin təhlükəsizliyini qorumaq şərti ilə bu iki maddənin dəyişdirilməsini istəmişdir. Ancaq Pentaqon əməliyyatların təhlükəsizliyini irəli sürərək protokolda dəyişiklik edilməsinə qarşı çıxmışdır. Nəticədə, protokola hər iki tərəfin bir tövsiyyə qərarı əlavə edilmişdir [15, 120].

Nyu-Yorkdakı Dünya Ticarət Mərkəzinə qarşı 2001-ci il sentyabrın 11-də baş verən hücumlardan sonra ABŞ, 2003-cü il, martın 20-də S.Hüseynin kütləvi qırğın silahlarına sahib olduğu və İraqın "Əl Qaidə"yə ev sahibliyi etdiyi iddialarını səbəb göstərərək, "terrorizmə qarşı mübarizə" ifadəsi çərçivəsində İraqa müharibə elan etdi.

Müharibənin əvvəlində Ağ Ev Səddam Hüseynin Birinci Körfəz müharibəsindən bəri həyata keçirdiyi dezinformasiya və təbliğatları izah edən hesabat yayımlamışdır. 2003-cü il, yanvarın 21-də "Təbliğat və Yalanların alətləri-Səddamın Dezinformasiya və təbliğatları" ("Apparatus of Lies Saddam's Disinformation and Propaganda") adlı hesabatda, Səddamın faciə yaratmaq üçün vətəndaşları hərbi birliklərin və hərbi sursatların yanında yerləşdirərək İraq xalqından qalxan kimi istifadə etdiyi, hərbi avadanlıqları məscid və digər mədəni abidələrin yaxınlığında yerləşdirdiyi, ölkənin aclıq və dərman çatışmazlığından əziyyət çəkdiyi, İslam dinini istismar etdiyi qeyd olunurdu [11, 103-104].

İkinci Körfəz müharibəsi zamanı, informasiya siyasəti, müharibə və media arasında yeni bir anlayış-"basdırılmış jurnalistika" ("Embedded journalism") anlayışı ortaya çıxarmışdır. "Basdırılmış jurnalistika" geniş mənada hərbi birliklərlə birgə hərəkət edən jurnalistlər mənasında istifadə olunur. "Basdırılmış jurnalistlər" hərbi birliklərlə birgə yaşayan, səyahət edən, yemək yeyən, yatan və bütün professional fəaliyyətlərdə onlarla birlikdə olan müxbirlərdir [27, 48].

İraq müharibəsi zamanı "basdırılmış jurnalistika"-nın əhatəsinə Fox, CNN, NBC və CBS kimi böyük televiziya kanalları ilə yanaşı USA Today, The New York Times, The Washington Post, The Washington Times və The Los Angeles Times kimi ən çox oxunan qəzetlər də daxil idi [13, 112].

"Basdırılmış jurnalistika" sistemində jurnalistlərin bitərəfliyi, ya da nə qədər azad şəkildə xəbər yayımlaya bilməsi başqa mövzudur.Əmrlərə qarşı gələn jurnalistlər "basdırılmamış" (disembedded) hesab olunmaqla evə geri göndərilirdi. Məsələn, döyüşdə ölən amerikalı əsgərin fotoşəklini nəşr edən "Time" xəbər agentliyinin cəbhədəki bütün müxbirləri geri göndərilmişdir.

ABŞ-ın mühafizəkar və respublikaçı baxışlara sahib ilk böyük televiziya kanalı kimi tanınan Fox televiziyası İraq müharibəsi zamanı vətənpərvər və milliyyətçi

yayımlarla xüsusilə ön plana çıxmış və ABŞ-da ən çox seyr edilən televiziya kanallarından biri olmuşdur.

İnformasiya müharibələrində ABŞ-ın iştirakından danışarkən, onun media koorporasiyalarının bu müharibələrdəki rolunu xüsusilə qeyd etmək lazımdır. I Körfəz müharibəsindən başlayaraq ABŞ-ın "CNN", "New York Times" kimi nəhəng media koorporasiyaları öz fəaliyyətini, nüfuz dairesini daha da genişləndirdi və rəqiblərindən bir addım önə çıxdı.

Son illərdə, medianın ABŞ-ın xarici siyasətinə və diplomatiyasına təsir göstərməsi nəticəsində "CNN effekti" adlanan nəzəriyyə formalaşdı. Bunun üçün iki əsas səbəbi qeyd etmək olar. Birincisi Soyuq müharibənin başa çatması, ikincisi isə texnologiyaların yüksək inkişafıdır. Ümumiyyətlə, belə nəticəyə gəlmək olar ki, ABŞ-ın media koorporasiyalarının informasiya müharibələrində fəal iştirakı onların qlobal təsirə malik olmasının sübutudur.

2.3. ABŞ-ın informasiya müharibələrinin onun xarici siyasətində yeri və rolu

"İnformasiya müharibəsi"nin geniş şəkildə həyata keçirilməsi I Körfəz Müharibəsi zamanı baş vermişdir. Bu termin o dövrdə ABŞ tərəfindən İraq informasiya sistemlərinin – hərbi və mülki informasiya vasitələrinin pozulmasına istiqamətlənmiş dezinformasiya və kinetik gücün tətbiqini nəzərdə tuturdu.

Bu gün dünyada supergüclərin apardıqları informasiya müharibələri onların xarici siyasətinə təsir göstərən əsas faktorlardan biridir. Bu sahədə əsas fəaliyyət göstərən aktorlardan biri də ABŞ-dır [2].

Son dövrlərdə Ağ ev dünya hökmranlığını təmin etmək üçün öz fəaliyyətində müxtəlif vasitələrdən istifadə edir və bu sahədə öz strategiyasını müəyyənləşdirir. Vaşinqton demək olar ki, dünyanın bütün nöqtələrində informasiyanın gizli yollarla əldə edilməsi, media yayımının idarə edilməsi və əhaliyə təsir göstərilməsi üçün

dövlətlərin sosial şəbəkələrinə hücum əməliyyatlarını reallaşdırır. Müdafiə üzrə Müasir Araşdırma Layihələri Agentliyində (DARPA) kiber sahədə hücum əməliyyatlarının aparılmasında ABŞ Müdafiə Nazirliyi üçün xüsusi "X Planı" hazırlanmışdır. Bundan əlavə, Birləşmiş Ştatların Milli Təhlükəsizlik Agentliyinin (MTA) Google, Yahoo, Facebook, Microsoft və digər meqa şirkətlərin məlumat mərkəzlərinə birbaşa çıxışı mövcuddur və kiber hücumlar çərçivəsində hazırlanmış proqramlarla kiber məkanın istənilən iştirakçısını rahatlıqla izləmək imkanına malikdir [2].

ABŞ-ın xüsusi xidmət orqanlarının fikrincə, rəsmi Pekin nəinki ABŞ-ın hərbi sirrlərini, onun Avropadakı müttəfiqlərinin sirrlərini də ələ keçirməyə davam edir. Halbuki ABŞ-ın xüsusi xidmət orqanının keçmiş analitiki Edvard Snoudenin də üzə çıxartdığı məxfi sənədlər sübüt edir ki, ABŞ hər yerdə "gözlərə və qulaqlara" malikdir. ABŞ-ın uzun illər ərzində hətta Almaniya kansleri Angela Merkelin telefon danışıqlarını dinlədiyi də aşkara çıxmış və bu iki ölkə arasında diplomatik qalmaqalla nəticələnmişdi. 2014-cü ilin iyulunun ortalarında Almaniya hökuməti casusluq fəaliyyəti ilə əlaqədar ABŞ səfirliyindən MTA-nın ölkə ərazisini tərk etməsini tələb etmişdir. Angela Merkellə yanaşı Fransa prezidenti Fransua Ollad, hətta Çexiya, Polşa kimi ölkələrin dövlət rəsmilərinin telefonları da ABŞ-ın xüsusi xidmət orqanları tərəfindən dinlənilmişdir [5].

"Wired Magazine" nəşrinə müsahibəsində Edvard Snouden qeyd edib ki, MTA-nın arsenalında "Mastermind" adlı silah mövcuddur. İnformasiya müharibəsinin aparılması üçün nəzərdə tutulmuş bu cihaz şəbəkə nəqliyyatının analizini apararaq, hücumların qarşısını almaq və onlara insan müdaxiləsi olmadan avtomatik cavab vermək funksiyası ilə təchiz olunmuşdur [2].

Son dövrlərdə verilən məlumatlara əsasən, ABŞ Rusiya, İŞİD (İraq Şam İslam Dövləti) və digər rəqiblərinə informasiya müharibəsində məğlub olur. Yeni yayılmış hesabatda ABŞ-ın təbliğat əleyhinə işi gücləndirməsi, hökumətin beynəlxalq yayım qanadına yenidən baxılması tövsiyə olunur."Reuters" agentliyinin əməkdaşı VarenStrobelyazır ki, bu hesabat 1994-cü ildə yaradılmış federal agentlik - Beynəlxalq Yayım Şurasının (BBG) problemlərinə işıq salır. 730 milyon dollar

büdcəsi olan BBG ABŞ hökumətinin radio, televiziya yayımını idarə edir. "Amerikanın Səsi", Azad Avropa/Azadlıq Radioları da buraya daxildir. "Reuters"in hesabatı 30 xarici siyasət və dövlət siyasəti peşəkarlarının dəyərləndirməsi əsasında hazırlanmışdır. Hesabat hökumətin maliyyələşdirdiyi yayımı ABŞ təbliğatına çevirməyi təklif etmir. Ancaq müəlliflərin fikrincə, bu yayım orqanlarını ABŞ-ın milli təhlükəsizlik qurumlarından ayıran sədd həddən artıq möhkəmlənib və onların yayımları heç də həmişə ABŞ-ın xarici siyasət hədəfləri ilə uyğunlaşmır.Hesabatda qeyd olunur ki, "ABŞ əleyhinə rəqiblər informasiya müharibəsi aparır, ABŞ-ın beynəlxalq yayımı da rəqibləri və media quruluşundakı dəyişikliklər ilə uyğunlaşmalıdırlar. ABŞ-ın beynəlxalq kommunikasiya strategiyası yenidən qurulmalı vəyeni hədəflər müəyyənləşdirilməlidir" [4].

BBG-nin keçmiş üzvü və Azadlıq Radiosunun keçmiş rəhbəri S.Enders Vimbuş qeyd edir ki, Ukrayna böhranı "Sovet İttifaqı dağılandan sonra ABŞ beynəlxalq yayımının üzləşdiyi ən böyük problemdir"[4].

BBG-nin Beynəlxalq Yayım Bürosunun direktor müavini Cef Trimbl vurğulayır ki, Rusiya Krıma girəndən əksəriyyəti rus dilində olmaqla 25 proqram ya yaradılıb, ya da genişləndirilib.

Agentlik Rusiyanın qarşısında tab gətirə bilmək üçün Konqresdən əlavə olaraq 15 milyon dollar ayırmasını istəyib. Konqres 2015-ci ildə büdcədən bu məbləğin ayrılması haqqında qərar qəbul edib. ABŞ rusdilli xidmətlərə ildə 20 milyon dollar vəsait xərcləyir[4].

Kiber hücumların vurduğu ziyan milyardlarla ölçülür. Müqayisə üçün qeyd etmək olar ki, Avropa İttifaqı kompüter viruslarının vurduğu ziyanı aradan qaldırmaq üçün ildə 12 milyard dollar vəsait xərclədiyi halda, ABŞ bunun üçün gündə 12 milyon , ildə isə 100 milyard dollar itirməli olur. ABŞ-da informasiya təhlükəsizliyinə qarşı olan təhdidlərin qarşısını almaq üçün "Kill Switch" adlı qanun qəbul olunmuşdur. Qanuna əsasən, ölkənin internet məkanına qarşı hər hansı xaker hücumu reallaşdırılarsa, mərkəzdən gələn tapşırığa əsasən prezidentin göstərişi ilə şəbəkəyə giriş bağlanacaq. Bu kiber hücumların qarşısını almaq üçün "Einstein-3" (Aynşteyn-3) adlı müdafiə proqramı yaradılmışdır. ABŞ-ın Milli Təhlükəsizlik

Nazirliyi tərəfindən yaradılmış bu proqramın köməyi ilə, ölkənin internet sisteminə xaricdən hər hansı yad müdaxiləyə dərhal reaksiya vermək və müdaxiləni zərərsizləşdirmək mümkündür [3].

ABŞ-ın informasiya müharibələrinin onun xarici siyasətinə necə təsir göstərməsi araşdırılması lazım olan əsas məsələlərdən biridir. Bu sahədə ABŞ-ın əsas rəqibləri olan Rusiya və Çinlə olan əlaqələrinə, onlarla apardığı informasiya müharibələrinə və bu müharibələrin onun xarici siyasətinə təsirinə xüsusilə diqqət yetirmək lazımdır.

İnformasiya müharibəsində ABŞ-ın ən böyük rəqibi Rusiyadır. Hər şeydən əvvəl ilk növbədə, Rusiya ilə ABŞ arasında əməkdaşlığı ehtiva edən fəaliyyətlərə diqqət yetirmək lazımdır. 2000-ci ilin ortalarında, ABŞ hüquq mühafizə orqanlarının səlahiyyətli nümayəndələri 6 kiber cinayətkarlıqla əlaqəli olan əməliyyatların birində rus həmkarlarından yardım aldıqlarını bildirdilər [37].

Rusiyanın kiber təhlükəsizlik agentlikləri ABŞ-da təlim keçmişdir [51]. Bu əmədaşlığın ən əhəmiyətli nümunələrindən biri 2006-cı ildə Şotlandiya Kral bankının ABŞ şöbəsindən 9 milyon dollar oğurlamaqda günahlandırılan Viktor Pleşçentanın ABŞ tərəfindən həbs olunmasıdır [37]. 2011-ci il iyunun 11-də Rusyanın Milli Təhlükəsizlik Nazirliyinin katibinin müavini tərəfindən idarə olunan heyət ABŞ-a səfər etdi. Səfər çərçivəsində hər iki ölkənin yüksək səlahiyyətli nümayəndələri iki ölkənin də qarşılaşdığı kiber təhlükəsizlik məsələləri ətrafında müzakirələr apardılar [69].

Keçmişdə mövcud olan bəzi əməkdaşlıqlara baxmayaraq, bir müddətdir ki, yenə də bu sahədə ABŞ Rusiya münasibətləri gərgindir. ABŞ-ın hüquq mühafizə orqanları Rusiyalı həmkarlarının kiber cinayətkarlıqla əlaqədar olan iddialara verilən cavablarının qeydsiz olduğunu və onlarla birlikdə bu sahədə ya çox az, ya da heç bir iş görmədiklərini düşünürlər. Daha da pisi isə budur ki, ABŞ-ın hüquq mühafizə orqanları rusiyalı kiber cinayətkarları həmkarlarına bildirmədən cəzalandırır və bu da Rusiya ABŞ münasibətlərinin daha da gərginləşməsinə gətirib çıxarır. 2000-ci ildə FTB (Federal Tədqiqatlar Bürosu) iki rus piratçısını iş təklifi ilə ABŞ-a dəvət edərək həbs etmişdir. FTB nümayəndləri, Rusiyanın Çelyabinsk şəhərində yaşayan iki

komputer piratçısının da komputerlərindən məlumatlar əldə etdilər. 2002-ci ildə Rusiya FTB əleyhinə Rusiyada fiziki olaraq mövcud olan komputerlərdən məlumatların oğurlanmasının qeyri qanuni olduğunu səbəb göstərərək, bu haqda cinayət işi elan edir. Eyni zamanda Rusiyanın səlahiyyətli nümayəndələri 2012-ci ildə rus vətəndaşı Vladimir Zdorovinin təhlükəsizlik korrupsiyasına, komputer quldurluğuna görə İsveçrə hüquq mühafizə orqanları tərəfindən ABŞ-a ekstradisiya edildiyində İsveçrə və ABŞ səlahiyyətlilərinin onlara xəbər vermədiyindən şikayətçi oldular.

Zdorovenin həbs olunmasında olduğu kimi, ABŞ üçün rusiyalı kiber cinayətkarları təqib etməyin bir yolu da onları müttəfiq ölkələrdən digər ölkələrə səfər edərkən tutmaqdır. Məsələn, Amazon.com-a və digər ABŞ-a aid olan elektron pərakəndə satış saytlarına 2008-ci ildə rus xaker tərəfindən hücum təşkil edilmiş, 2012-ci ilin iyul ayında bu xaker Kiprdə həbs olunmuşdur [67].

Putin tərəfdarları ABŞ əleyhinə olan mühafizəkarlardan ibarətdir [76]. ABŞ-ın İraqa müdaxiləsi zamanı istifadə etdiyi informasiya texnologiyaları, müharibədən sonrakı dövrdə Rusiyanın ona qarşı açıq düşmənçiliyini dilə gətirməsinə səbəb oldu. 2012-ci ildə Rusiyada keçiriləcək prezident seçkiləri iləəlaqəli təşviqat kompaniyalarının birində Putin çıxış edərkən öz nitqində "Bəzən ABŞ-ın müttəfiqlərə ehtiyacı olmadığını hiss edirəm" deyə bildirdi [70].

Rusiya və ABŞ bəzi cinayətlərin araşdırılması üçün sazişlər imzalasalar da, bu sazişlərin içində kiber cinayətlərləəlaqəli heç bir müddəa yoxdur. 2001-ci ildə ABŞ-ın Ədliyyə Nazirliyi (Department of Justice) rusiyalı həmkarlarından kömək tələb etdi, lakin cavab almadı. Rusiya kiber cinayətlərləəlaqədar qarşıdurmaları həll etmək üçün beynəlxalq hüquqa da müraciət etdi. Buna ən gözəl nümunə kimi yuxarıda qeyd olunmuş 2002-ci ildə Rusiyadakı komputerlərdən məlumatların oğurlanması səbəbilə Rusiyanın FTB əleyhinə beynəlxalq hüquqa müraciət etməsini göstərmək olar [48, 15]. Rusiyanın BMT-nin Təhlükəsizlik Şurasındakı nümayəndəsi Nikolay Patruşey qeyd etmişdir ki, "Beynəlxalq hüquq çərçivəsində bu məsələnin həllini tapmaq asan vəzifə deyil, çünki bunun üçün heç bir norma və qayda yoxdur" [47].

ABŞ Milli Kəşfiyyat İdarəsinin direktoru Ceyms Klepper, 8 noyabrdakı prezident seçkisindən əvvəl Rusiyadan yönələn kiber hücumları ABŞ-da seçkilərə edilən "ən təcavüzkar müdaxilə"saymışdır. ABŞ Senatının Silahlı Qüvvələr Komitəsində, kiber hücumlar üçün açılan istintaq çərçivəsində ifadə verən Ceyms Klepperöz çıxışında "Hücumlar ABŞ hökumətinə böyük təhdid meydana gətirdi" deyəqeyd etdi. Klepper, Rusiyanın kiber hücumlarının səslərin siyahıya alınmasında təsirinin olmadığını söylədi.

ABŞ kəşfiyyat xidmətləri tərəfindən komitəyə təqdim edilən hesabatda, Rusiyanın kiber hücumlar vasitəsilə Respublikaçı namizəd Donald Trampın prezident seçilməsinə kömək etdiyi vurğulanaraq günahlandırılırdı.

Demokratik Milli Komitənin e-poçt hesabı da hücuma məruz qalmışdır. Prezident seçkilərindən əvvəl, Respublikaçı namizəd Donald Trampla mübarizədə məğlubiyyətə uğrayan demokrat namizəd Hillari Klintonun seçki kampaniyasını icra edən Con Podestanın e-poçtları xaker hücumuna məruz qalmışdı. Podestanın yazışmaları Vikiliksdə paylaşılmışdı.

Günahlandırmalar ABŞ ilə Rusiya arasında diplomatik gərginlik yaratdı. ABŞ35 rus diplomatı kompüter piratçılığı yolu ilə prezident seçkilərinə müdaxilə etdiklərini iddia edərək sərhəddən xaric etmişdi. İttihamları rədd edən Kreml isə kiber hücum iddiaları üçün "ədəbsizlik" ifadəsindən istifadə etmişdi. Donald Trampın qrupundan da bəzi adlar kəşfiyyat orqanlarının şərhlərinə şübhəilə yanaşaraq "Bunlar, Səddam Hüseynin kütləvi qırğın silahları olduğunu iddia edənlərlə eyni insanlardı" deyə qeyd etmişdilər [9].

NBC News kanalına müsahibə verən ABŞ kəşfiyyatının səlahiyyətli nümayəndələri, Obama administrasiyasının Rusiyaya kiber sahədə cavab vermək üçün MKİ-nin səlahiyyətli nümayəndələrinə lazım olan işləri görməsi üçüm təlimat verdiyini iddia etdi [10].

Telekanal bildirir ki, Amerikanın vəzifəli şəxsləri çoxdandır Rusiya, Çin və digər ölkələrin Birləşmiş Ştatların mühüm infrastruktur obyektlərinin proqram təminatına virus yeritmək üçün cəhdlər göstərib. Artıq ABŞ da düşmənlərə qarşı eyni taktikanı işə salıb. Kanala daxil olan sənədlərə əsasən, ən azından Rusiyaya qarşı belə

əməliyyat keçirilib. Çünki Amerika rəsmiləri Rusiyanın ABŞ prezidenti seçkilərinin nəticələrinə kiber-hücumlarla müdaxiləsi ehtimalından narahatdır. ABŞ-ın kiber-komandanlığının keçmiş müşaviri, ehtiyatda olan polkovnik Harri Braun deyib ki, Amerika Milli Kəşfiyyat Agentliyinin xarici ölkələrdəki kompyuter şəbəkələrinə haker hücumları sonradan kiber-silah üçün platsdarm yaratmaq üsuluna çox oxşayır: "Siz şəbəkəyə çıxış əldə edirsiniz, orada öz iştirakınızı təmin edib sonra istədiyinizi etmək imkanları qazanırsınız. Əvvəlcə siz informasiyaları toplayırsınız, amma həmin çıxış imkanlarını daha aqressiv hərəkətlər üçün də istifadə edə bilərsiniz". ABŞ kəşfiyyatındakı yüksək rütbəli mənbə deyib ki, Rusiya Birləşmiş Ştatların strateji infrastrukturuna qarşı irimiqyaslı kiberhücum həyata keçirməyə cəhd etsə, buna cavab olaraq Rusiyanın bir çox sistemləri sıradan çıxarılacaq [9].

Obama, radioda verdiyi müsahibədə seçkilərə qarşı yönələn müdaxilənin açıq olduğunu söylədi. “Aydındır ki, Rusiya tərəfindən edilən hücumlar Klintonun seçki kampaniyası üçün Trampın seçki kampaniyası ilə müqayisədə daha böyük problemlər yaratdı” deyə Obama qeyd etdi[19].

ABŞ-ın kiber sahədə ən böyük rəqiblərindən biri də Çindir. İlk olaraq, Çin ilə ABŞ arasında bəzi əməkdaşlıqların mövcud olduğunu qeyd etmək lazımdır. 2011-ci ilin əvvəlində Çinin səlahiyyətli nümayəndələri və ABŞ-ın FTB (Federal Təhlükəsizlik Bürosu), uşaq pornoqrafiyası iləəlaqədar qeyri qanuni veb saytın bağlanılması üçün ortaq əməliyyatlar təşkil etmişdilər. Müvəffəqiyyətli əməkdaşlığın bu nümunəsinə baxmayaraq, onlar arasında kiber təhlükəsizlik sahəsində də bir sıra ziddiyyətlər mövcuddur.

Bəzi Qərb analitikləri Çini, dövlətlərin daxili işlərinə qarışan, sərbəst şəkildə fəaliyyət göstərən xaker qrupları formalaşdırmaqda günahlandırırlar. Çin isə Qərbdəki iddialara cavab olaraq, ABŞ hökümət təşkilatlarının kiber cinayətkarlıqla mübarizə aparmaqdan və çinli həmkarları iləəməkdaşlıq etməkdən boyun qaçırdığını qeyd etdi. İctimai Təhlükəsizlik Nazirliyinin şəbəkətəhlükəsizliyiniqoruma bürosunun müdir müavini olan Gu Jean, Çinin saxta bank veb saytları və uşaq pornoqrafiyası kimi kiber cinayət mövzularında 13 dəfə ABŞ-dan əməkdaşlıq tələb etsələr belə, cavab almadıqlarını ifadə etdi[46].

Son dövrdə baş verən hadisələr Çinin və ABŞ-ın bu sahədə bir-birini günahlandırmaqla məşğul olduğunu göstərir. 2013-cü il iyunun 5-də Çin gündəlik qəzetinin dərc etdiyi məqalədə qeyd olunur ki, "Çin ABŞ-dan ona qarşı yönələn ciddi kiber hücumların hədəfinə çevrilib, lakin Pekin Vaşinqtonu və ya Pentaqonu heç zaman "texniki olaraq məsuliyyətsiz"dir, deyə günahlandırmadı..." [86].

ABŞ və Çin arasında bu sahədəəməkdaşlıqla yanaşı çatışmazlıqlar da mövcuddur. Xüsusilə "Snouden hadisəsi"ndən sonra Çin hökuməti ABŞ-a qarşı daha qəzəbli və düşməncəsinə bəyanatlar irəli sürmüşdür. Çinin mobil şirkətləri ciddi sürətdə bu məsələdə narahat olduqlarını qeyd etdilər[57].

Ümumiyyətlə, Çin hökuməti ABŞ-dan ona qarşı yönələn kiber hücum təhlükəsi altında olduğunu düşünür. Çin siyasətçiləri Microsoft və ABŞ hökümətinin birgəəməkdaşlıq edərək, çinli komputer istifadəçilərinin Microsoft məhsullarındakı gizli hesablarına nəzarət etdiyini vurğulayırlar. Bu səbəbdən də, çinli texniklər, ABŞ və onun müttəfiqi olan ölkələrdən idxal edilən komputer və komputer proqramlarını nəzarət altına alır, Qərb mütəxəssislərinin proqramlara nəzarətinə qarşı müqavimət göstərirlər [48, 13].

Çinli kriptoqrafçılarının bildirdiyinə görə "Microsoft" məhsullarında ABŞ-ın Milli Təhlükəsizlik Agentliyi (National Security Agency) iləəlaqəli olan "NSA Açarı" tapılmışdır. ABŞ hökümətinin Microsoft Windows 95, 98, N-74 və 2000-ə birbaşa girişi olduğu iddia edilir. Microsoft bu iddianı rədd edib problemi həll etmək üçün cəhdlər göstərsə belə, Çin hökuməti bununla razılaşmamışdır. Çinin 14 böyük yüksək səviyyəli texnologiya şirkətləri Qərb ölkələrində ticarətdə və investisiya yatırmaqda bənzər maneələr ilə qarşı-qarşıya qalmışdır. Lenovo İBM-in PC hissəsini alan çinli PC istehsalçısı köhnə şirkətin Çin hökuməti ilə olan əlaqəsinə görə böyük manelərlə qarşılaşmışdır. ABŞ-ın bəzi millət vəkilləri qeyd etdilər ki, bu razılaşma nəticəsində sonradan şirkətin digər texnologiyaları da Çin hökumətinin nəzarətinə keçə bilər. Bu tənqidlər, 2006-cı ildə Lenovo şirkətinin ABŞ-ın Xarici İşlər Nazirliynə 16000 masaüstü komputer satmaq istədiyi vaxtda yenidən ortaya çıxdı. Şirkətin Çin hökuməti ilə olan əlaqəsi səbəbindən, siyasətçilər və bəzi şərhçilər, Çin kompüterlərinin ABŞ-ın hökumət binalarına yerləşdirilməsinin milli təhlükəsizliyə

hədə olduğunu vurğuladı. Digər yüksək texnologiya şirkəti olan Hauwey də, Avstraliya, Hindistan və ABŞ-da buna bənzər maneələrlə üzləşdi [48, 14].

Son dövrlərdə ABŞ Dövlət Departamenti bir sıra bəyanatlar vermişdir. Bu bəyanatlara əsasən,ABŞ-ın hər il bir mühüm həyati sahəsi iflic olur.Çinin "xaker ordusu" ilk dəfə ABŞ xəstəxanalarına və ordu qərargahının məxfi hissələrində saxlanılan gizli sənədlərə qısa yolla daxil ola bilmişlər. Nəticədə 370 milyonluq ABŞ əhalisinin bəlkə də hamısının məlumatlarını oğurlamışlar. Çinin "xaker ordusu"nun bu cür hücumları nəticəsində Çin hərbi texnologiya sahəsində 25 ildə əldə edə biləcəyi uğuru 1 ildə qazandı, bununla yanaşı milyardlarla dollar əldə etdi.

Çin 2012-ci ildə ABŞ-ın ikinci ən böyük xəstəxanasına xaker hücumu təşkil etmişdir. Bu hücum nəticəsində xəstəxananın arxivində mövcud olan 4,5 milyon xəstənin təhlükəsizlik nömrələri, ünvan və digər məxfi məlumatları ələ keçirildi. Əldə olunan dəlillər FTB-ə təqdim edildi. Uzun zaman ötsə də, MKİ bu haqda heç bir açıqlama vermədi. Məlumatlara görə, bu hücum Çinin "Anonimus" xaker qrupu tərəfindən reallaşdırılmışdır [3].

Çin xakerləri 18 milyon şəxsin sosial nömrəsini ələ keçirmişdir. Eyni zamanda Con Kerri, Hillari Klinton və ABŞ dövlətinin əsas rəhbərlərinin bütün gizli informasiyaları da ələ keçirilən məlumatlar arasındadır.

Pekinin "Tiananmen" meydanında 1989-cu il iyunun 4-də baş vermiş qanlı tələbə qiyamının 25-ci il dönümündən əvvəl Google-a giriş qadağan edilmişdi. İnternetdə senzura və qadağalara nəzarət edən GreatFire.org saytına görə Çin Google-un axtarış mühərrikinə və e-mail xidmətinə girişə maneə törədərək, onları yararsız hala gətirmişdi. 2010-cu ildə Çindəki xidmətini bağlayan Google, Hong Kong əhalisinə xidmət etməyə davam edir. Son olaraq 2012-ci ildə Google-a 12 saatlıq giriş qadağan olunmuşdur. Facebook, Twitter və Google-un sahib olduğu Youtube 2009-cu ildən bəri Çində qadağan edilmişdir.

FTB-nin məxfi hesabatlarında göstərilir ki, Çinin 80 min virtual casusdan ibarət ordusu mövcuddur. Bu kiber ordu ABŞ üçün olduqca böyük təhlükədir. Belə ki, bu ordu, ABŞ-ın həyati vacib infrastruktur obyektlərini məhv etməyə, bank işini və kommersiya əməliyyatlarını pozmağa, həmçinin hərbi və müdafiə strukturlarının

gizli məlumat bazalarına daxil olmağa qadirdir. Çinin kiber ordusu tərəfindən son bir neçə il ərzində ABŞ-ın Müdafiə Nazirliyinin kompüterlərinə 90 min dəfə hücum təşkil olunmuşdur. Çinin hərbi strateqləri hərbçilər içərisində virtual casusluqla məşğul olmaq üçün 30 min nəfərə xüsusi təlim keçməyə başlamışlar. Bundan əlavə, özəl sektordan olan 150 min çinli kompüter eksperti müşavir, təlimçi, proqramçı kimi bu layihəyə cəlb edilmişdi. Çinli xakerlər ABŞ-ın Müdafiə Nazirliyinin kompüter şəbəkəsinə 2007-ci ildə 44 min, 2008-ci ildə 55 min, 2009-cu ildə isə 90 min dəfə hücumetmişdir. Çinin İctimai Təhlükəsizlik Nazirliyi informasiya müharibəsi sahəsində minlərlə bölmələrə malikdir və 140 milyon internet istifadəçisinin qoşulduğu daxili trafik bütünlüklə bu nazirliyin nəzarəti altındadır [3].

"Microsoft" şirkəti Çində öz biznesini qurarkən özünün "Office" proqram təminatı paketinin gizli kodlarını Çin hökumətinə məcburən təqdim etmişdi, amma buna baxmayaraq Çinin dövlət planlaşdırması üzrə komissiyası "Microsoft Windows" əməliyyat sistemini, ABŞ hökumətinin kəşfiyyat məlumatları toplamaq üçün gizli aləti elan etdi [14]. Çin tərəfindən "Microsoft" şirkətinə bildirildi ki, "Windows" proqramına Çinin öz kodlarını yerləşdirmək üçünçinli proqramçılar hazırlamasa, o, burada fəaliyyət göstərə bilməyəcək. Gəliri əsas tutan "Microsoft" şirkəti bu şərtlə razılaşmaq məcburiyyətində qaldı.O, xüsusi kodlarla işləməyi bacaran çinli proqramçıları yetişdirməyə məcbur oldu. Bunun nəticəsində də Çinin hərbi kəşfiyyatı, xakerlərin jarqonuna uyğun "kilidaçan" əldə etməyi bacardı. Hal-hazırda Çin mütəxəssisləri dünya səviyyəsində proqramların təməlində duran kodları yaratmaq qabiliyyətinə malikdirlər. Bu kodların ilk sınağı ABŞ Dövlət Departamentinə, Ticarət Nazirliyinə, Hərbi Dəniz kollecinə və həmçinin, FTB-nin özünün komputer sistemlərinə hücumlarla başladı. Artıq çinli xakerlər yeni vasitələrə əl atmağa başlayıblar. Onlar kompüter şəbəkələrinə "informasiya minaları" (soxulcanlar) yerləşdirirlər[3].

ABŞ-ın Milli Təhlükəsizlik Agentliyinin 2007-ci ildə 1,8 milyard dollar məbləğində olan kompüter şəbəkəsi çinli xakerlər tərəfindən sındırılmış və Çin vebsaytına sayı məlum olmayan informasiya ötürülmüşdür. Çin tərəfindən gələ biləcək təhlükələr ABŞ istifadəçilərini o qədər qorxudur ki, ABŞ-ın Çində fəaliyyət

göstərən “İntel” kompüter şirkətinin məhsullarına ABŞ-ın özündə etibar edilmir. Çinin müxtəlif vaxtlarda Tayvana qarşı reallaşdırdığı kiber hücumlarda ABŞ, Tayvana ən böyük və real dəstək verən ölkə hesab olunur [3].

Bütün bu sadalananlardan əlavə ABŞ-ın xarici siyasətinə mənfi təsir göstərən amillərdən biri də “Snouden hadisəsi” olmuşdur. “Snouden hadisəsi” (Snowden Case) olaraq dünya ictimaiyyətinin gündəminə hakim olan bu hadisədə kəşfiyyat dünyası ilə, MTA (National Security Agency) vasitəsilə tanış olan və daha sonra da CİA-də çalışan 30 yaşındakı Eduard Snouden adlı bir ABŞ vətəndaşının adı ilə bağlıdır.Bu hadisənin digər casusluq və ya məlumat sızdırma hadisələrindən fərqi budur ki, Snouden dövrümüzdə daha çox kiber casusluq iləəlaqəli olan dövlətlərarası kəşfiyyat mübarizəsini açıq şəkildə nümayiş etdirən ilk agentdir. Edvard Snouden, CİA-nın texniki işlər üzrə keçmiş mütəxəssisi olub.

Cenevrədə diplomatik nümayəndə kimi vəzifəsini icra edən E. Snouden agent olduğu müddətdə, gördüklərini və yaşadıqlarını xalqa izah etməyə və ABŞ-ın həyata keçirdiyi kəşfiyyat üsullarını ictimaiyyətə çatdırmağa qərar vermişdir. Snouden, B.Obamanın da kəşfiyyat sahəsində islahatlar həyata keçirmədiyini gördükdə bu qərarını tətbiq etmiş və2013-ci ildən etibarən mediaya məlumat sızdırmağa başlamışdır. 2009-ci ildə MTA-ya bağlı olan xüsusi firmalarla çalışmağa başlayan Eduard Snouden “The Guardian” qəzetinin müxbiri Glin Grinvalda ABŞ-ın kəşfiyyat metodları haqqında məlumat sızdırmağa başlamışdır[25].Honq Konqa gedərək “The Guardian” qəzetini axtararan E. Snouden onlara müsahibə vermək istədiyini bildirmişdir. Snouden baş tutan ilk görüşdə yalnız mövzunun səthi qismi haqqında məlumatlar verdi. “The Guardian” qəzeti iyunun 6-da Snoudendən aldığı məlumatları nəşr etməyə davam etmişdir. İyunun6-da nəşr olunan məlumatlarda MTA-nin Google, Facebook, Apple və digər ABŞ şirkətlərinin məlumatlarına birbaşa çıxışını təmin edən “Prism” adlı proqram haqqında söz açmışdır. Bu proqramı inkar edən sözü gedən şirkətlər yalnız ABŞ hökumətinin məhdud girişinə icazə verdiklərini bəyan etmişlər. İyunun 7-də açıqlama vermək məcburiyyətində qalan Barak Obama bu iki proqramı müdafiə etmiş və təhlükəsizliklə şəxsi həyat arasındakı tarazlığa maksimum diqqət yetirdiklərini ifadə etmişdir [23, 26].

İyunun 9-da Snouden xalqa xitabən video müsahibə hazırlamışdır. Bu müsahibədə E. Snouden: "Özümdə danışmamaq ehtiyacı hiss etmirəm. Çünki səhv etdiyimi düşünmürəm"-deyərək MTA-nın "Prism" proqramı haqqında ətraflı məlumat vermişdir. Snouden 12 iyun tarixində Honq Konqdaki "South China Morning Post" qəzetinə müsahibə verərək MTA-nın 2009-ci ildən bəri Çin kompüterlərinə daxil olaraq onlara məxsus məlumatları əldə etdiyini söyləmişdir.

İyul ayında "Snouden hadisəsi" təqribən otuza qədər ölkənin də daxil olduğu beynəlxalq xarakter almışdır. Bolivya prezidenti Evo Morales Snoudenə dəstək verərək maskaların artıq düşməyinin lazım olduğunu vurğulamışdır. Bu sözlərə görə Boliviya prezidentinin təyyarəsinin diplomatik toxunulmazlığı aradan qaldırılmış və onun təyyarəsi Moskva-La Pas səfərində Vyanaya eniş etmək məcburiyyətində qalmışdır. Bundan sonra da təyyarə yoxlanışdan keçirilmişdir. Avropa ölkələri bu təyyarənin ölkəsinə dönməsinə icazə vermədilər. Bundan əlavə, Fransa, Portuqaliya və İspaniya da Evo Moralesin onların hava sahəsindən istifadəsini qadağan etmişdir. Bunun səbəbi isə Vashington tərəfindən axtarılan E. Snoudenin təyyarədə olması ehtimalı idi. Hadisənin baş verdiyi ərəfədə Boliviya prezidenti qaçaq kəşfiyyat işçisi iləəlaqədar vəziyyəti şərh edərək siyasi sığınacaq tələbini nəzərdən keçirəcəyini söyləmişdir. Bir çox Avropa dövlətlərinin liderləri Boliviya prezidentinin bu ifadəsinəəsaslanaraq Moralesin Snoudeni Rusiyadan qeyri-qanuni yolla aparmaq qərarına gəldiyinə inanırdılar. Boliviya hökuməti dövlət başçısının Vyana hava limanında gözlədilməsi və təyyarəsinin axtarılmasıməsələsini Birləşmiş Millətlər Təşkilatında (BMT) müzakirəyə çıxarmışdır. Bundan sonra iyulun 3-də BMT-nin baş katibi Pan Gi-Mun öz çıxışında, Snoudenin malik olduğu rəqəmsal məlumatlardan səhv istifadə etdiyini və ictimai xeyirdən daha çox problemlərin ortaya çıxmasına səbəb olduğunu ifadə etmişdir [23, 26]. Bu şərhindən üç gün sonra, əvvəl Venesuela prezidenti Nikolas Maduro, sonra da Nikaraqua prezidenti Daniel Orteqa Snoudenə humanitar sığınacaq verə biləcəklərini ifadə etmişdir [43]. Bütün bunlar baş verərkən əvvəl iyulun 20-də "The Guardian" ofisindəki kompüterlər yox edildi və sonra isə avqustun 18-də Glen Grinvaldın iş yoldaşı David Miranda "Heathrow Hava Limanı"nda həbs olundu [68]. Hazırda Snouden Rusiyadan

sığınacaq alaraq orada yaşayır. CNN-nin verdiyi məlumata əsasən Snouden hazırda Rusiyada veb saytlarının yaradılması işi ilə məşğul olur[41].

İnformasiya müharibələrində ABŞ-ın iştirakının onun xarici siyasətinə təsiri çox böyükdür. Xüsusilə, Rusiya və Çin kimi böyük rəqiblərlə apardığı informasiya müharibələri ABŞ xarici siyasətinə təsir göstərən əsas faktorlardan biridir. Kiber təhlükəsizlik sahəsində bu dövlətlər əməkdaşlıqdan daha çox rəqabət apararaq informasiya məkanında üstünlüklərini təmin etməyə çalışırlar. Rusiya və Çin tərəfindən ABŞ-a kiber hücumların təşkil edilməsi ölkələrarası münasibətlərdə gərginliyə səbəb olur. Almaniya, Fransa kimi inkişaf etmiş Avropa dövlət başçılarının telefon danışıqlarının dinlənilməsini ortaya çıxaran "Snouden hadisəsi"ndən sonra Rusiyanın Snoudene sığınacaq verməsi iki ölkə arasındakı münasibətlərin daha da kəskinləşməsinin sübutudur.

NƏTİCƏ

Nəticə etibarilə qeyd etmək lazımdır ki, informasiya müharibələri dünya dövlətlərinin diqqət mərkəzində olan əsas məsələ və buna qarşı mübarizə XXI əsr dünya dövlətləri qarşısında duran əsas vəzifələrdəndir. Qeyd olunduğu kimi, "İnformasiya Müharibəsi" anlayışı ilk dəfə ABŞ-da meydana gəldi və daha geniş şəkildə məhz bu məkanda araşdırıldı. Bu isə İnformasiya Kommunikasiya Texnologiyalarının ABŞ-da geniş şəkildə inkişafı və tətbiqi ilə əlaqədardır. İnformasiya müharibəsi üzrə mütəxəssis Martin Libiki bu müharibənin əhəmiyyətini xüsusilə qeyd etmiş və müharibənin gələcəyi haqqında düşünməyin qaçınılmaz olduğunu vurğulamışdır. M. Libiki ilk dəfə bu müharibənin 7 əsas formasını təsnifatlandırmış və müharibədə istifadə olunan texnologiyalar arasındakı əlaqələri göstərmişdir. Qeyd olunan təsnifata əsasən, bura komanda-nəzarət, kəşfiyyat, elektron, psixoloji, xaker, iqtisadi və kiber müharibələr aiddir.

Beynəlxalq mühitin getdikcə mürəkkəbləşməsi, yeni maraqların yaranması ölkələrin yeni strateji hədəflər müəyyənləşdirməsinə səbəb oldu. Yeni hədəflər bir tərəfdən beynəlxalq mühitdə stabilliyin ve sabitliyin qorunmasına yönəlmişdisə də, digər tərəfdən ölkələrin daha çox informasiyaya hakim olma marağına yönəlmişdi. Çünki dövlətlər artıq yaxşı başa düşürdülər ki, XXI əsrdə informasiya kimin əlindədirsə, güclü tərəf məhz odur. İnformasiya müharibəsinin yeni forması olan "strateji informasiya müharibəsi"nin isə daha az xərc tələb etməsi, müasir informasiya texnologiyalarının istifadəsi baxımından daha əlverişli olması, informasiya müharibələrində iştirak edən ölkələrin fəal mübarizəsinə səbəb oldu.

2001-ci il 11 sentyabr terror hadisələri ABŞ-ın yeni informasiya siyasətinin formalaşması üçün dönüş nöqtəsi oldu. Məhz bu hadisələrdən sonra "kiber təhlükəsizlik" 2002-ci il və ondan sonrakı illərdə qəbul olunan Milli Təhlükəsizlik Strategiyalarının əsas tərkib hissəsinə çevrildi. Müasir dövrdə də davamlı olaraq texnologiya dünyasının dəyişməsi və inkişafı ilə təhdidlərin də sayı artmaqda davam edir. Bu təhdidlərin qarşısını almaq üçün isə qanunvericilikdə daima onlarla mübarizə yolları axtarılır.

Əslində geosiyasi mühitdə dəyişiklik "Soyuq müharibə"dən sonra başladı. "Soyuq müharibə"nin başa çatması ilə, yeni geosiyasi sistem formalaşdı, hərbi taktika və strategiyalarda köklü dəyişikliklər baş verdi. Belə ki, müdafiəyə ayrılan xərclərin azalması, texnologiyaların sürətli inkişafı XXI əsrin əvvəllərində terror hadisələrinin və qarşıdurmaların artması sosial-iqtisadi vəziyyətlə yanaşı yeni hərbi yanaşmalara ehtiyac olduğunu sübut etdi. Bu dövrdə ABŞ-da "Silahlı qüvvələrin şəbəkə strukturu və ya şəbəkə müharibəsi" adlı yeni konsepsiya yarandı. ABŞ Silahlı qüvvələrində şəbəkə strukturunun yaradılması bir sıra texnologiyaların inkişafını tələb edir. Bu texnologiyalara peyklər, pilotsuz aparatlar, nanotexnologiyalar, kompüter prosessorları və b. daxildir. Texnologiyaların sürətli inkişafı mütəmadi olaraq ABŞ silahlı qüvvələrində də şəbəkə struturunun yenilənməsinə, yeni plan, taktika və strategiyaların hazırlanmasına gətirib çıxarır.

İnformasiya müharibələrində ABŞ-ın iştirakından danışarkən, onun media koorporasiyalarının bu müharibələrdəki rolunu xüsusilə qeyd etmək lazımdır. I Körfəz müharibəsindən başlayaraq ABŞ-ın "CNN", "New York Times" kimi nəhəng media koorporasiyaları öz fəaliyyətini, nüfuz dairesini daha da genişləndirdi və rəqiblərindən bir addım önə çıxdı.

Son illərdə, medianın ABŞ-ın xarici siyasətinə və diplomatiyasına təsir göstərməsi nəticəsində "CNN effekti" adlanan nəzəriyyə formalaşdı. Bunun üçün iki əsas səbəbi qeyd etmək olar. Birincisi Soyuq müharibənin başa çatması, ikincisi isə texnologiyaların yüksək inkişafıdır. Ümumiyyətlə, belə nəticəyə gəlmək olar ki, ABŞ-ın media korporasiyalarının informasiya müharibələrində fəal iştirakı onların qlobal təsirə malik olmasının sübutudur.

İnformasiya müharibələrində ABŞ-ın iştirakının onun xarici siyasətinə təsirinin önəmini də qeyd etmək lazımdır. Xüsusilə, Rusiya və Çin kimi böyük rəqiblərlə apardığı informasiya müharibələri ABŞ xarici siyasətinə təsir göstərən əsas faktorlardan biridir. Kiber təhlükəsizlik sahəsində bu dövlətlər əməkdaşlıqdan daha çox rəqabət apararaq informasiya məkanında üstünlüklərini təmin etməyə çalışırlar. Rusiya və Çin tərəfindən ABŞ-a kiber hücumların təşkil edilməsi ölkələrarası münasibətlərdə gərginliyə səbəb olur. Almaniya, Fransa kimi inkişaf

etmiş Avropa dövlət başçılarının telefon danışıqlarının dinlənilməsini ortaya çıxaran “Snouden hadisəsi”ndən sonra Rusiyanın Snoudene sığınacaq verməsi iki ölkə arasındakı münasibətlərin daha da kəskinləşməsinin sübutudur.

Bütün qeyd olunanlar onu deməyə əsas verir ki, xüsusilə XXI əsrdə İnformasiya Kommunikasiya Texnologiyalarının sürətli inkişafı, inkişaf etmiş ölkələrin bu texnologiyaları əldə etmək istəyi sonda onların mübarizəsi ilə nəticələnir. İnformasiya texnologiyalarının həm istehsalında, həm də istehlakında fərqlənən ABŞ-ın bu müharibələrdə iştirakı və əldə etdiyi üstünlük, onun qlobal hegemonluğunu təmin etməsi istiqamətində həyata keçirdiyi fəaliyyətin əsas tərkib hissələrindən biridir.

Bu gün Amerika Birləşmiş Ştatları informasiya məkanında və eləcə də informasiya siyasətində kifayət qədər güclü rəqiblərinin olmasına baxmayaraq hegemon dövlət statusunu qoruyub saxlayır.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISI

Azərbaycan dilində:

1. Ələkbərova İ.Y. İnformasiya Müharibəsi Texnologiyalarının Analizi Və Təsnifatı // İnformasiya cəmiyyəti problemləri. 2010, №2, s. 80-91
2. Əliyeva Z. Kiber məkanda Qərb-Şərq qarşıdurması, Bakı: 17 mart 2015 //http://newtimes.az/az/cyberspace/3391/
3. Həsənov F. Kiber Savaş: ABŞ təklənir –Təhlil, 20 sentyabr 2016 //http://femida.az/news.php?id=37905
4. Nabiullina E. ABŞ-ın informasiya müharibəsini Rusiyaya uduzmağı // Azad Avropa/Azadlıq Radiolarının studiyası. 27 mart, 2015 //https://www.azadliq.org/a/26923553.html
5. Nurəddinoğlu R. ABŞ-ın Avropanı gizli dinləməsi..., 7 iyul 2015 //http://sia.az/az/news/economy/487892-abs-in-avropani-gizli-dinlemesi
6. Talışınski E. İnformasiya Müharibəsinin Aktuallığı Və Onun Sosial-Psixoloji Təhlili // AMEA Şərqşünaslıq İnstitutu, 23 fevral 2009 //http://www.azhumanrights.az/
7. Vaşinqton Post, 6 fevral 2010 //http://mediaforum.az/articles .php?lang=az&page=02&article_id=20100406103443296#.WMQoF6L-vIU
8. Vəliyeva A. İnformasiya müharibəsi: "Heç kim əsgər deyil, lakin hamı döyüş iştirakçısıdır" // Azərbaycan Respublikası Rabitə və Yüksək Texnologiyalar Nazirliyinin Məlumat Hesablama Mərkəzi, 2 dekabr 2015 //http://rabitadunyasi.info.az/News/?newsID=7 79&lang=az

Türk dilində:

9. ABD istihbaratı: Rusya'nın siber saldırıları büyük tehdit. 5 Ocak 2017 //http://www.bbc.com/turkce/haberler-dunya-38518573
10. ABD ve Rusya arasında siber savaş! 31 Aralık 2016 //http://www.yeniakit.com.tr/

11. Akıner N. Düşman Değiliz: 11Eylül'ün Ardından Amerikan Milliyetçiliği. İstanbul: Karakutu Yayınları, 2001, 220 s.
12. Alagöz E. A. Amerikanın yeni güvenlik stratejisi // Bilge Adamlar Strateji Araştırmalar Merkezi. 18 Şubat 2015 //http://www.bilgesam.org/
13. Can F. Bilgi Çağının Güdümlü Silahı Medya. İstanbul: Alfa Yayıncılık, 2005, 224 s.
14. Enformasyon Savaşı için Ağır Silahlanma, //http://www.bianet.org/
15. Gökdağ R. Amerikan Medyasında 11 Eylül. İstanbul: E Yayınları, 2001, 222 s.
16. Güngör M. Ulusal Bilgi Güvenliği: Strateji ve Kurumsal yapılanma. T.C Kalkınma Bakanlığı, Bilgi toplumu Dairesi Başkanlığı, Yayın No: 2919 Mart 2015. 143 s.
17. İlhan E., Dirik N. Savaş Haberleri Bağlamında Haber Politikaları: ABD Örneği. Güz 2011, Sayı: 33 s. 26
18. Kılıç B. K. -"Önleyici Savaş ile "Stratejik Sabır" arasında ABD-nin Ulusal Güvenlik stratejisi, Seta Perspektiv dergisi, Sayı: 90 19 Şubat 2015. s. 7
19. Mazlumoğlu A. E. ABD ile Rusya arasında siber düello. 16 Aralık 2016 //http://medyascope.tv/2016/12/16/abdile-rusya-arasinda-siber-duello/
20. Mevlutoğlu A. Ağ merkezli muharebe üzerine notlar-II: Durumsal Farkındalık. 13 eylül 2010 //http://www.siyahgribeyaz.com/2010/09/ag-merkezli-muharebe-uzerine-notlar-ii.html
21. Mutlu M. Vietnam'dan Körfez'e Savaşlarda Kamuoyu Oluşumu. İstanbul: Okumuş Adam Yayınları, 2003, 390 s.
22. Sağsan M. Bilgi Savaşı: Siperlerden Klavyelere Taşınan Harekâtın Anatomisi // Avrasya Dosyası, İstihbarat Özel, Yaz 2002, Cilt: 8, Sayı: 2, s. 213-232
23. Sezgin F. Edward Snowden Olayı'nın ABD-Rusya İlişkileri Üzerindeki Etkileri. Uluslararası Yönetim ve Sosyal Araştırmalar Dergisi, ISSN:2148-1415, 2014, s. 24-31
24. Taylan D. Ana-akım Medyayı Ana-akım Medya Yapan Nedir? Z Medya Enstitüsü'nde Yapılan Konuşma //http://bgst.org/medya-ve-yayincilik/ana-

akim-medyayi-ana-akim-medya-yapan-nedir-z-medya-enstitusunde-yapilan-konusma

25. Tüysüzoğlu G. Post-Modern Bir Casusluk Hikayesinin Kahramanı: Edward Snowden. 15 Temmuz 2013 //http://blog.milliyet.com.tr/post-modern-bir-casusluk-hikayesinin-kahramani--edward-snowdeb/Blog/?No=422385
26. Ünver M., Canbay C. Kritik altyapıların korunması. Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı Mayıs 2010. 34 s.
27. Yalçınkaya H. Savaşlarda Asker-Medya İlişkilerinin Geldiği Son Aşama: İliştirilmiş Gazetecilik. 5 Mart 2011, s. 30-54

Rus dilində:

28. Абдурахманов М.И., Баришполец В.А., Баришполец Д.В., Манилов В.Л., Геополитика, международная и национальная безопасность // Словарь-справочник / Под общей редакцией В.Л. Манилова, "Пробель", Москва. 1999. с. 127-130
29. Бедрицкий А. В., Информационная война: концепции и их реализация в США// Российский институт стратегических исследований, Москва. 2008. 187 с.
30. Бедрицкий А. В., Современная концепция информационной войны- Москва. 2007. с. 86-113

İngilis dilində:

31. Alain D., New Secrets // Paris, SEDES, 1967, 405 p.
32. Alberts D. S., Garstka J. J. Network Centric Warfare: Developing and Leveraging Information Superiority. 2nd edition (revised), August 1999/Second printing February 2000. 287 p.

33. Arquilla J., Ronfeldt D., Zanini M. Networks, Netwar, and Information-Age Terrorism // The Changing Role of Information in Warfare. Rand Corporation. 1999. p. 88–89
34. Adams J. Virtual defense // Foreign AffairsMay/June:98-112. 2001 //https: //www.foreignaffairs.com/articles/2001-05-01/virtual-defense
35. Bill of Rights of the United States of America (1791). Amendment I //http://www.billofrightsinstitute.org/
36. Belknap M. H. The CNN Effect: Strategic Enabler or Operational Risk? // Usawc Strategy Research Project, 30 March 2001, 33 p. //http://www.iwar.org.uk/
37. Bryan-Low C. Digital trails: in Eastern Europe, a gumshoe chases internet villains; Microsoft deploys Mr. Fifka to hunt cyber felons amid rise in online crime; tailing 'Benny' in a Czech city. Wall Street Journal, A.1 September 1, 2005
38. Colonel A. D., Douglas H. Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Hardcover) // Afcea Intl Pr, 2000, p. 309.
39. Denning D. Information Warfare and Security // Addison-Wesley, 1999, p.9-19.
40. E-Government Act of 2002. Pub.L. 107-347 //https://www.it.ojp.gov/
41. Eshchenko A. Edward Snowden Gets Website Job in Russia, Lawyer Says. November 1, 2013 //http://edition.cnn.com/2013/10/31/world/europe/russia-snowden-job/
42. FISMA Background // http://csrc.nist.gov/groups/SMA/fisma/overview.html
43. Gidda M. Edward Snowden and the NSA files files – Timeline, 23 June, 2013 //https://www.theguardian.com/
44. Gray C. Another Bloody Century – Future Warfare, 2005. 143 p.
45. İnformation Security. National Institute Standarts and technology: U.S. Department of Commerce, 2010. 94 p.
46. Internet policing hinges on transnational cybercrime, China Daily, November 10, 2010 //http://www.china.org.cn/

47. Isachenkov V. Putin: Snowden must stop leaking secrets to stay. Associated Press, Monday, July 1, 2013 //http://www.washingtontimes.com/
48. Kshetri N. Cybersecurity and International Relations: The U.S. Engagement with China and Russia. The University of North Carolina at Greensboro, Argentina, July 23-25, 2014.38 p.
49. Kuehl D. T. Information Operations, Information Warfare, and Computer Network Attack Their Relationship to National Security in the Information Age // İnternational Law Studies, p. 36-58
50. Lewis B.C. Information Warfare //https://fas.org/
51. Libicki M. What is Information Warfare? // National Defense University, ACIS, August 1995. 104 p.
52. Liu Y. Q. The impact of national policy on developing information infrastructure nationwide issues in P:R: China and the U.S. Libri, 1996, 175-183.
53. Livingston S. Clarifying The Cnn Effect: An Examination of Media Effects According to Type of Military Intervention. Harvard University John F. Kennedy School of Government, Cambridge: 18 June 1997, MA 02138, p. 21
54. Meade C., Cassidy S. FISMA Updated and Modernized. December 19, 2014 //https://www.insidegovernmentcontracts.com/
55. Menyhért K. Military Adaptation of Protected İnformation Systems, p. 91-99 //http://hadmernok.hu/archivum/2007 /3/2007_3_kerner.pdf
56. Military Information Technology Online Edition. Interview with Major General Steven W. Boutelle. 2003 //http://www.military-information-technology.com/article.cfm?DocID=33
57. Miriam E., Kaiman J. Putin: NSA whistleblower Snowden is in Moscow airport, The Guardian//https://www.theguardian.com/
58. Molander R.C., Riddle A. S. Strategic Information warfare: A New Face of War //http://www.rand.org/pubs/monograph_reports /MR661/index2.html

59. Moscaritolo A. Prison sentence for RBS hacker suspended in Russia. September 09, 2010 // https://www.scmagazine.com/prison-sentence-for-rbs-hacker-suspended-in-russia/article/558124/
60. Muir A., Oppenheim C. National Information Policy developments worldwlde II: universal access-adressing the digital divide // Journal of Information Science, 2002b, 236-273 p.
61. Oates S. Introduction to Media and Politics. SAGE Publications, London: 2008, p. 21
62. Office of Force Transformation (OFT). The Implementation of Network Centric Warfare. Document 387, 2005 //http://www.oft.osd.mil/
63. Office of Force Transformation // http://www.oft.osd.mil
64. Rona T. Weapon Systems and Information War. Office Of The Secretary Of Defense, Washıngton Dc: 1 July 1976. p. 71
65. Ross R., Swanson M. Information Security. National Institute Standarts and technology, USA: Department of Commerce 2004. p. 69
66. Rothkopf D. Rice Pudding // Foreign Policy, 6 February 2015 //http://foreignpolicy.com/2015/02/06/rice-pudding/
67. Russian Hacker Arrested in Cyprus Over U.S. Attacks, RIA Novosti, 20 July, 2012 // https://sputniknews.com/world/20120720174690453/
68. Savage C. Britian Detains The Partner of a Reporter Tied To Leaks. AUG. 18, 2013 //http://www.nytimes.com/2013/08/19/world/europe/britain-detains-partner-of-reporter-tied-to-leaks.html
69. Schmidt H. U.S. and Russia: Expanding the "Reset" to Cyberspace. July 12, 2011 //https://obamawhitehouse.archives.gov/blog/2011/07/12/us-and-russia-expanding-reset-cyberspace
70. Shuster S. Putin Turns His Back on Snowden — and His Own Anti-Americanism, July 02, 2013 //http://world.time.com/2013/07/02/putin-turns-his-back-on-snowden-and-his-own-anti-americanism/
71. Sites by region //http://www.voanews.com/navigation/allsites

72. Stupples D. The next war will be an information war, and we're not ready for it // City University London, World Economic Forum, November 27, 2015 //https://www.weforum.org/agenda/2015/12/what-is-information-warfare/
73. Swartz J. Cybercriminals can't get away with it like they used to // USA Today, November 17, 2008
74. The DoD Cyber Strategy, The Department of Defence, Washington DC: 17 April 2015, 42 p.
75. The Future of Information Warfare, SANS Institute InfoSec Reading Room. USA: SANS Institute, 2001, p. 10
76. The Kremlin's new Anti-Americanism, 16 September 2013 //http://www.economist.com/
77. The Media in the United States. U.S. Diplomatic Mission to Germany /Public Affairs/ Information Resource Centers //https://usa.usembassy.de/
78. The National Security Strategy, The White House Washington: May 2010, p. 60
79. The National Security Strategy, The White House Washington: February 2015, 35 p.
80. The National Security Strategy of the United States of America, The White House, Washington: September 2002, 35 p.
81. The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets, The White House, Washington: February 2003, 96 p.
82. The National Strategy to Secure Cyberspace, The White House, Washington: February 2003, 76 p.
83. Toffler A., Toffler H. War and Anti-War. Little, Brown and Company, Boston: 1993, 302 p.
84. U.S. Government IT Security Laws. SANS Institute InfoSec Reading Room 2004, p. 29 //https://www.sans.org/
85. Who Controls The Media? // http://www.theglobalmovement.info/wp/areas-of-focus/global-financial-war/who-controls-the-media

86. Xiaokun L. China is victim of hacking attacks. June 05, 2013 // http://en.people.cn/90883/8271052.html

87. 6th International Conference on Information Warfare and Security, The George Washington University, Washington, USA: 17-18 March 2011, //http://academic-conferences.org/

88. 100th Congress. Computer Security Act of 1987., 1988 //https://www.congress.gov/bill/100th-congress/house-bill/1158

89. 104th Congress. Informatıon Technology Acquısıtıon Pılot Programs. Feb. 10, 1996, p. 679-703 // https://www.dol.gov/ocfo/media/regs/ITMRA.pdf

90. 108th Congress. Informatıon Security, 2003, p. 72 //https://sdsos.gov/services-for-individuals/assets/h218enr.pdf

91. 112th Congress 2d Sessıon In The Senate Of The Unıted States February 14, 2012 // https://www.congress.gov/bill/112th-congress/senate-bill/2105