UOT 004.351

Ələkbərova İ.Y.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
depart17@iit.ab.az

İNFORMASİYA MÜHARİBƏSİ TEXNOLOGİYALARININ ANALİZİ VƏ TƏSNİFATI

Məqalədə informasiya müharibəsi texnologiyalarının yaranma səbəbləri və bununla əlaqədar meydana çıxan problemlər araşdırılmış, müxtəlif mütəxəssislərin və alimlərin "informasiya müharibəsi" terminina münasibətləri təhlil edilmişdir. İnformasiya müharibəsi texnologiyalarının təsnifatı verilmiş, informasiya təsiri problemləri analiz edilmişdir. İnformasiya müharibəsinin istiqamətləri və hədəfləri göstərilmişdir.

Açar sözlər: *İnformasiya müharibəsi, kibermüharibə, informasiya silahı, informasiya qarşıdurması, kompyuter cinayətkarlığı, elektron müharibə, haker, informasiya-texniki təsir, informasiya-psixoloji təsir, informasiya hücumu.*

Giriş

Dünyada cərəyan edən proseslər hər bir dövlətin ən başlıca vəzifələrindən birinin onun öz informasiya məkanına nəzarəti gücləndirməklə, informasiya resurslarının mühafizəsi uğrunda mübarizə aparmalı olduğunu söyləməyə əsas verir. Son zamanlar bir çox dövlətlər öz vətəndaşları və iqtisadi maraqlarının təhlükəsizliyi ilə yanaşı, mədəni-mənəvi dəyərlərini qorumaq üçün xüsusi tədbirlər görmək məcburiyyətindədirlər. Bu baxımdan, dövlətlər konseptual səviyyədə məqsədlərini həyata keçirmək, siyasi, iqtisadi və hərbi sahələrdə müvəffəqiyyət əldə etmək üçün vacib olan informasiyanı əldə etməyə çalışırlar.

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 (bank-maliyyə, nəqliyyat, elektrik şəbəkələri, neft və qaz xətləri) tətbiq edilməsi isə onları informasiya müharibəsində potensial obyektlərə çevirmişdir.

İnformasiya texnologiyalarının inkişafı ilə əlaqədar daha asan və tez əldə edilən informasiya dövlətin və cəmiyyətin özünü ifadə etməsi baxımından ideal vasitə hesab olunur. Bu səbəbdən, son zamanlar iqtisadiyyatda, siyasətdə və hərbi sahədə "informasiya əməliyyatı" (*Information Operation*) və "informasiya müharibəsi" (*Information Warfare*) terminləri geniş istifadə edilir. Dünyada informasiya müharibəsi (İM) texnologiyalarının inkişafı və dövlətlər arasında baş verən hərbi və siyasi qarşıdurmalar belə söyləməyə əsas verir ki, yaxın gələcəkdə qarşı tərəf üzərində üstünlük informasiyanın ələ keçirilməsi, onlara çevik reaksiya verilməsi, real vaxt rejimində qarşı tərəfin informasiya mənbələrinin məhv edilməsi ilə əldə olunacaqdır.

Bu gün cəmiyyətdə milli informasiya resurslarının mühafizəsi məsələsi çox aktualdır. İnkişaf etmiş dövlətlər tərəfindən informasiya silahının (*Information Weapon*)

tətbiqi və qlobal informasiya infrastrukturunun yaradılması bu ölkələrin dünyada lider olmaq iddiasından irəli gəlir. İnternet açıq informasiya şəbəkəsinin genişlənməsi, kompyuter cinayətkarlığının artması, siyasi və iqtisadi məqsədlərə çatmaq üçün yüksək səviyyədə informasiya hücumu təhlükələrinin çoxalması informasiya müharibəsi və informasiya təhlükəsizliyi kimi məsələlərin aktuallığına səbəb olmuşdur.

İKT-nin inkişafı və informasiya müharibəsi

İM və onun tətbiqi texnologiyalarının kökü qədim dövrlərə gedib çıxır. Bəşər tarixində informasiya təcavüzü bu və ya digər formada hər zaman olmuşdur. Belə ki, insanların informasiyasız yaşamaları mümkün deyil. Fiziki müharibə aparmadan İM aparmaq olur, amma İM olmadan fiziki müharibə aparılmır. Başqa sözlə, fiziki müharibə aparılarkən, eyni zamanda, onun tərkib hissəsi kimi İM-in aparılması zəruridir. Məsələn, Çingiz xanın hərbi yürüşləri zamanı ordunun önündə xüsusi informasiya hazırlığı görmüş müəyyən qrup atlılar çapırdılar. Onlar Çingiz xanın opdusunun hədsiz dərəcədə güclü və amansız əsgərlərdən təşkil olunduğu haqqında xəbərlər yayaraq əhalidə qorxu, ruh düşkünlüyü yaradırdılar. Bu cür psixoloji təsir üsullarından digər məşhur sərkərdələr (Makedoniyalı İsgəndər, Teymurləng və s.) tərəfindən də istifadə edilmişdir. Həmçinin II Dünya müharibəsi zamanı Hitler və Stalin də informasiya-psixoloji təsirin əhəmiyyətini yaxşı anlayırdılar [1]. O zamankı informasiya əməliyyatlarının indiki analoji əməliyyatlardan yeganə fərqi o idi ki, həmin dövrlərdə informasiyanın ötürülməsində texniki vasitələrdən istifadə edilmirdi.

Müasir dövrdə informasiyanın emalı və ötürülməsində istifadə edilən maddi-texniki bazanın inkişafı ilə İM-in tətbiqi və texnologiyaları köklü şəkildə dəyişmiş, informasiya şəbəkəsinin yaranması və geniş yayılması İM-in əhəmiyyətini artırmışdır. Bu gün İM problemləri informasiya kommunikasiya texnologiyalarının (İKT) inkişaf etdiyi bir çox ölkələrdə (ABŞ, Rusiya, İngiltərə, Fransa, İsveçrə, Yaponiya və s.) araşdırılmaqdadır.

Müasir İM texnologiyalarının yaranması, inkişafı və geniş tətbiqinin müxtəlif izahları var:

1. Hesablama texnikası və kommunikasiya vasitələrinin sürətli inkişafı, şəbəkə texnologiyalarının təkmilləşdirilməsi cəmiyyətdə əsas resurs kimi informasiyanın rolunun artmasına səbəb oldu.
2. Effektivliyinə görə informasiya maddi resurslardan daha yuxarıda dayanmağa başladı. Elmi-texniki nailiyyətlər hərbi sahədə istifadə edilən ənənəvi silahlarla yanaşı, bir sıra İKT vasitələrinin kütləvi istehsalına şərait yaratdı.
3. İnsanların beyinlərinin və davranışlarının öyrənilməsində əldə edilən nailiyyətlər müxtəlif istiqamətlərdə psixofizioloji təsirlərin yollarını və vasitələrini daha yaxşı başa düşməyə imkan verdi.

“İnformasiya müharibəsi” termini haqqında

İM probleminin obyektiv və müfəssəl təhlilini aparmaq üçün qabaqcıl ölkələrin təcrübəsi, xarici mütəxəssislərin, alimlərin, praktiklərin fikirlərinin öyrənilməsi və müqayisəsi tələb olunur. ABŞ-da İM problemi son 15 ildə digər ölkələrlə müqayisədə daha geniş araşdırılmış və öyrənilmişdir. Bunu ABŞ rəsmi dairələrinin, o cümlədən Müdafiə Nazirliyinin, Konqresin rəsmi sənədlərində, rəsmi şəxslərin açıq bəyanatlarında, İM problemləri ilə məşğul olan təşkilatların hesabatlarında görmək mümkündür.

İlk dəfə “informasiya müharibəsi” terminini 1976-cı ildə amerikalı mütəxəssis

Tomas Rona (*Thomas Rona*) "*Boeing*" şirkəti üçün hazırladığı "Silah sistemləri və informasiya müharibəsi" adlı hesabatında istifadə etmişdir. T.Rona hesabatında sübut etmişdir ki, son illərdə informasiya infrastrukturu ABŞ iqtisadiyyatının əsas komponentinə çevrilmişdir [2].

"İnformasiya müharibəsi" termini rəsmi olaraq ilk dəfə ABŞ Müdafiə Nazirliyinin 21 dekabr 1992-ci il tarixli, 3600.1 saylı direktivində istifadə edilmişdir [3].

İM-in ilk tədqiqatçılarından biri, ABŞ-ın Milli Müdafiə Universitetinin əməkdaşı Martin Libiki (*Martin Libicki*) İM anlayışına tərif verərkən demişdir: "İnformasiya müharibəsini bütün incəliyi ilə anlamaq təşəbbüsü kor adamların fili tanımaq üçün göstərdikləri cəhdləri xatırladır: filin ayağına toxunan onu ağac, quyruğuna toxunan adam onu kəndir adlandırır və s. Bu üsulla tam təsəvvür almaq mümkündür? Ola bilsin ki, fil yoxdur, həqiqətən də, ağac və kəndir vardır. Bir qrup mütəxəssis bu anlayış altında bir çox istiqamətləri birləşdirmək istədikləri halda, digərləri informasiya müharibəsinin hər-hansı bir aspektini ümumi anlayış kimi qəbul edir..." [4]. M.Libiki bu fikri ilə demək istəyirdi ki, "informasiya müharibəsi" çox geniş anlayışdır və İM texnologiyalarının cəmiyyətə təsiri tam aydınlaşdırılmasa da, son illər bu proses sürətlə davam etməkdədir.

ABŞ-ın Müdafiə Nazirliyinin İM haqqında sənədlərində bildirilir ki, İM-də informasiya həm silah, həm də məqsəddir. İnformasiya hücumu isə icazə olmadan istənilən formada informasiyanın köçürülməsi, dəyişdirilməsi və məhvinə, həmçinin proqram təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatdır [5].

ABŞ-da İM-i təsvir etmək üçün çox zaman onu informasiya əməliyyatı ilə müqyisə 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 həyata keçirilən mübarizə formasıdır [6]. Rusiya mütəxəssisləri 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 göstərə bilir [7].

Amerika tədqiqatçılarının fikrincə, informasiya əməliyyatı vasitələrilə realizə olunan informasiya qarşıdurması hərbi qüvvələrin, elmi mərkəzlərin, müxtəlif siyasi təşkilatların hazırlığında və fəaliyyətində İM texnologiyalarından geniş istifadəni nəzərdə tutur [8].

İnformasiya qarşıdurmasında əsas məqsəd qarşı tərəfin informasiya da daxil olmaqla, bütün növ resurslarına təsir göstərməkdir. İnformasiya qarşıdurmasının effektivliyinin əsas meyarı kimi qarşı tərəfə məxsus 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. üsullar geniş istifadə edilir. Qeyd etmək lazımdır ki, İM prosesində kompyuter şəbəkəsinə daxil olmaqla, həmçinin İnternet vasitəsi ilə qarşı tərəfin mühüm əhəmiyyət kəsb edən maliyyə, bank sistemi, rabitə, elektrik təchizatı və nəqliyyat vasitələrini iflic etmək mümkündür. Bu məqsədlə İnternetdə veb-briqadalar və hakerlər fasiləsiz işləyirlər. Onlar xüsusi təşkil edilmiş, fəaliyyətləri müəyyən hədəflərə yönəldilmiş peşəkarlardır. İM-də həmçinin informasiya-kommunikasiya sistemlərinin normal iş fəaliyyətinin pozulması, psixoloji-ideoloji

informasiyanın, şayiələrin yayılması, informasiya blokadası, yayılması və s. informasiya əməliyyatlarından geniş istifadə edilir.

İM sahəsində aparılan araşdırmalar nəticəsində məlum olmuşdur ki, İM nəzəriyyəsinin tədqiqatı ilə məşğul olan alimlər üç əsas qrupa bölünürlər:

- Birinci qrup alimlər İM texnologiyalarını ayrı-ayrı informasiya əməliyyatı və informasiya rəqabəti vasitələrinə, dövlətlərarası münaqişələrin, silahlı mübarizələrin aparılmasına, kütləvi şüura təsir texnologiyalarına uyğunlaşdırırlar (sosial-kommunikativ yanaşma) [9, 10, 11, 12, 13].
- İkinci qrup alimlərə hərbi mütəxəssislər aiddir. Onların fikrincə, İM hərbi münaqişələrlə birbaşa bağlıdır və bu münaqişələrə informasiya-hərbi mübarizə vasitələrinin və gücün kompleks birgə tətbiqi kimi baxılmalıdır (hərbi-tətbiqi yanaşma) [14, 15, 16]. Bir çox mütəxəssislər bu yanaşma ilə razılaşmır və bildirirlər ki, "informasiya müharibəsi" termini hərbi əməliyyatların aparılması zamanı müasir informasiya texnologiyalarına münasibətdə hər zaman adekvat olmur və bu növ hərbi əməliyyatları "informasiya mübarizəsi" və ya "informasiya qarşıdurması" adlandırmaq daha düzgün olardı [17, 18, 19].
- Üçüncü qrupa aid tədqiqatçılar İM ilə bağlı əməliyyatlara dövlətlərarası münaqişələrdən yaranan hadisə kimi baxırlar. Onların fikrincə, dövlətlər arasında yaranan siyasi münaqişələri hərbi yolla deyil, müasir İKT vasitələrindən istifadə etməklə həll etmək mümkündür. Bu baxımdan, bir çox tanınmış alimlər İM-i geosiyasi münaqişəyə aid edərək, ona dövlətlər arasında xüsusi münasibət növü kimi baxırlar. Onların fikrincə, mövcud münaqişəni aradan qaldırmaq üçün bu ölkənin informasiya mühitində müxtəlif güc təsirlərinin metod, vasitə və texnologiyaları tətbiq olunmalıdır (geosiyasi yanaşma). Bu qrup mütəxəssis İM zamanı əməliyyatların zorakılıq xarakterini qabardaraq, onu açıq hərbi əməliyyatların aparılmadığı şəraitdə belə müharibənin ən vacib və təhlükəli əlaməti hesab edirlər [20]. Belə tədqiqatlar bir daha sübut edir ki, artıq dünyada tətbiqi elmin yeni sahəsi – İM nəzəriyyəsi inkişaf etməkdədir.

İnformasiya müharibəsi texnologiyaları

Son illərin lokal müharibələri və silahlı münaqişələri hərbi mütəxəssisləri informasiya vasitələrinin hərbi sistem və komplekslərə effektli təsirlərinin qlobal analizini aparmağa məcbur etmişdir. İM hər bir dövlətin daxilində, ilk növbədə, hakimiyyət və pul, insanları idarə etmək imkanı əldə etmək uğrunda, eləcə də, istehsalat məhsullarına nəzarət və onun realizə olunmasında əldə edilən gəlir uğrunda aparılır. Müxtəlif mütəxəssislər və alimlər tərəfindən İM-ə müxtəlif təriflər verilsə də, hər kəs təsdiq edir ki, İM, əsasən, hakimiyyət və kapital uğrunda müharibədir.

İM bilik uğrunda – "nə?", "nə zaman?", "harada?", "nə üçün?" və "nə dərəcədə?" suallarına cavab tapmaq uğrunda müharibədir. İM-i son məqsəd hesab etmək olmaz, o yalnız vasitədir. İM sahəsindəki təcrübələr, vasitələr və metodlar yalnız hərbi-siyasi sahədə deyil, dövlətin iqtisadi maraqlarında geniş istifadə olunur və əsas məqsəd qarşı tərəfin informasiya resurslarının ələ keçirilməsinə, informasiya sistemlərinin məhv edilməsinə yönəlmişdir.

M.Libiki 1995-ci ildə ABŞ-ın Milli Müdafiə Universiteti tərəfindən nəşr edilmiş "İnformasiya müharibəsi nədir?" məqaləsində ilk dəfə İM texnologiyalarının təsnifatını vermişdir. Bu konsepsiyada ilk dəfə olaraq göstərilmişdir ki, son dövrlərdə İKT-nin

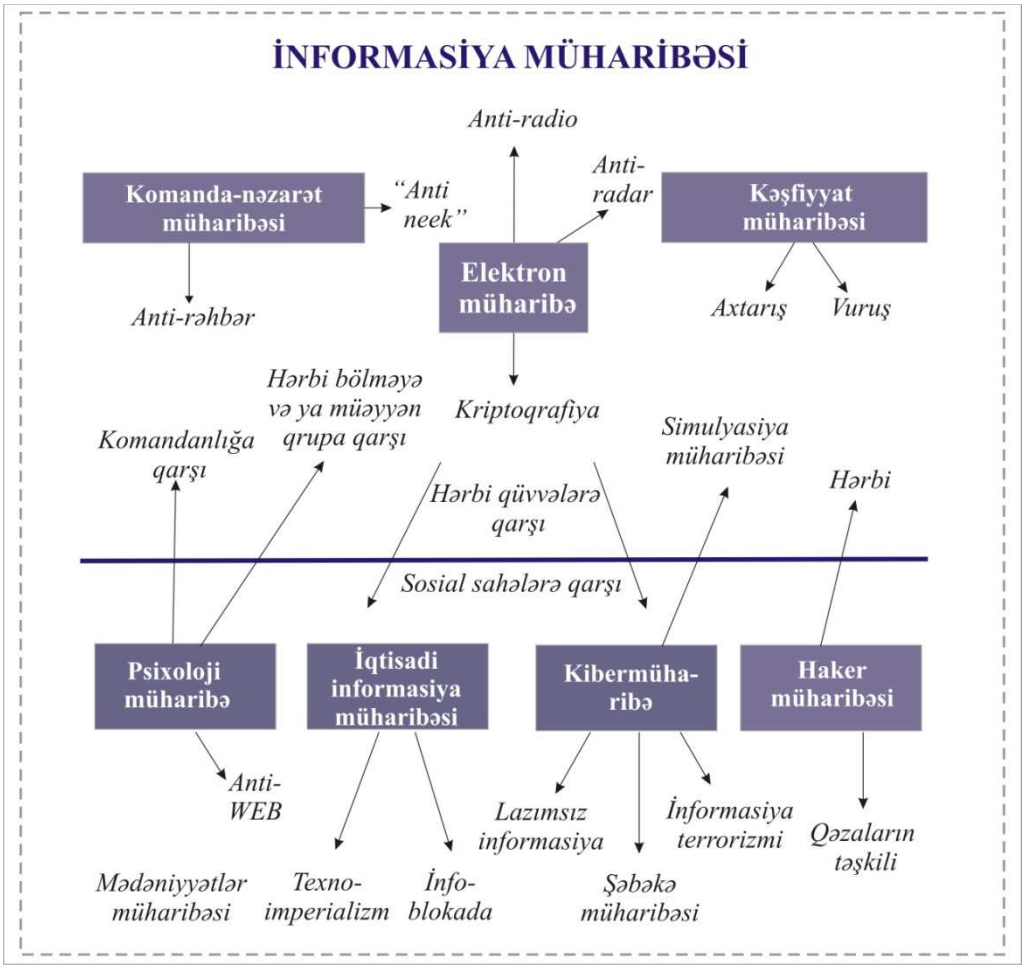
inkişafı nəticəsində artıq İM-də psixoloji deyil, əsasən, iqtisadi və hərbi aspektlərə üstünlük verilir. M.Libikinin fikrincə, izləyici kosmik peyk şəbəkəsindən yerüstü, dəniz və hava məkanında baş verən dəyişiklikləri qeyd edən sistemlərdən ibarət əlaqəli informasiya sistemləri dünyada baş verən istənilən hərbi aktivliyi nəzarətdə saxlamaq imkanına malik olacaqdır. Bu isə sistemə həmin aktivliyi iflic etmək və onun iqtisadi və informasiya sistemlərini dünyadakı digər sistemlərdən ayırmaq imkanı verəcəkdir. Bu konsepsiya informasiya silahından aktiv istifadənin kosmik vasitələrin tətbiqi ilə sıx əlaqəli olduğunu bir daha sübut etmiş oldu.

M.Libiki "İnformasiya müharibəsi nədir?" məqaləsində İM-in yeddi formasını qeyd etmiş, "*Information Warfare*" adlanan sistemdə texnologiyalar arasında əlaqələri göstərmişdir (şəkil 1).

Bu texnologiyalara, əsasən, komanda-nəzarət, kəşfiyyat, elektron, psixoloji, haker, iqtisadi, kibermüharibə aiddir:

1. ***Komanda-nəzarət müharibəsi*** *(Command and Control Warfare)* – komandanlıq və icraçılar arasındakı əlaqə kanallarına istiqamətlənmiş İM-dir. Bu əlaqə kanallarının funksiyası pozularsa, İM-də qələbənin təmin olunması reallaşar. Komanda nəzarət müharibəsində "antinik" (*anti-neek*) adlanan əməliyyatlara daha çox önəm verilir ki, bunun da mənası lazımsız, avara müdaxilələrə qarşı tədbirlər deməkdir.
2. ***Kəşfiyyat müharibəsi*** *(Information Based Warfare)* – mühüm informasiyanın toplanması və bu zaman hücum edən tərəfin öz informasiya resurslarını mühafizə etməsi prosesidir.
3. ***Elektron müharibə*** *(Electronic Warfare)* – elektron kommunikasiya vasitələrinə qarşı yönəlmiş müharibədir. Elektron kommunikasiya vasitələri dedikdə, radioəlaqə, radarlar, kompyuter şəbəkəsi nəzərdə tutulur. Onun əsas bölməsi kriptoqrafiyadır (elektron informasiyanın şifrələnməsi və ya şifrədən çıxarılması).
4. ***Psixoloji müharibə*** *(Psychological Warfare)* – təbliğat, "beyinlərin yuyulması", əhalinin davranışlarına nəzarət və vətəndaşlar üçün nəzərdə tutulmuş informasiyanın emalıdır. M.Libiki psixoloji müharibəni 4 hissəyə ayırır: 1) Vətəndaş ruhunun sarsıdılması; 2) Hərbi qüvvələrdə mənəvi duruma və əhval-ruhiyyəyə nəzarət; 3) Komandanlığa dezinformasiyanın ötürülməsi; 4) Mədəniyyətlərin müharibəsi (*War of Culture*).
5. ***Haker müharibəsi*** *(Hacker Warfare)* – qarşı tərəfin mülki obyektlərinə yönəlmiş diversiya əməliyyatlarıdır. M.Libiki haker fəaliyyətlərindən danışarkən 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, hakerlərin silahı viruslardır – "troyan atları", məntiqi bombalar, sniferlər (izləyiçilər), şəbəkə soxulcanları və s. Tədqiqatçı hakerləri ABŞ üçün ciddi təhlükə hesab edir və bu fikrini onunla əsaslandırır ki, digər ölkələrlə müqayisədə Amerikada müxtəlif lokal və qlobal şəbəkələrdən istifadə praktikası daha genişdir. M.Libiki ikimənalı olaraq göstərir ki, Amerika universitetlərində informasiya texnologiyaları sahələri üzrə müdafiə edən doktorantların 60%-ni əcnəbilər təşkil edir ki, onların da 2/3 hissəsi müsəlman ölkələrindən və Hindistandan gələnlərdir.
6. ***İqtisadi informasiya müharibəsi*** *(Economic Info-Warfare)* – M.Libiki bu müharibəni iki formada təsvir edir: informasiya blokadası (ABŞ-a qarşı yönəlmiş) və

informasiya imperializmi və ya texno-imperializm (ABŞ tərəfindən). İnformasiya blokadası dedikdə, ilk növbədə, informasiya və ticarət əlaqələrinin kəsilməsi (fiziki ticarətə qadağanın qoyulması) nəzərdə tutulur. Bank şəbəkələrinin sındırılması bu kateqoriyaya daxil deyil və haker fəaliyyəti hesab olunur. İnformasiya imperializmi ümumi iqtisadi imperializm siyasətinin bir hissəsidir. M.Libiki bildirir ki, ticarətin özü də müharibədir.



Şəkil 1. M. Libiki tərəfindən təqdim edilən "İnformasiya müharibəsi sxemi"

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

8. ***Simulyasiya müharibəsi*** *(Simulation Warfare)* – real döyüş meydanındakı hərbi əməliyyatların kompyuter modeli ilə əvəz olunmasıdır. Məsələn, təyyarəçilər səmaya qalxmadan döyüş təcrübəsi əldə etmək üçün fayl-simulyatorlarda işləyirlər

("vuruşurlar"). Simulyasiya müharibəsi, əsasən, nümayiş effekti yaradır və dünyanın virtuallaşmasının əyani nümunəsidir. Dünyanın virtuallaşması, daha doğrusu, dünyanın kompyuter versiyasının yaradılması ona gətirib çıxaracaq ki, gələcəkdə simulyasiya müharibəsi real müharibə ilə eyni məna kəsb edəcək və bir statusda olacaqdır.

İlk dəfə 1993-cü ildə Con Arkuilla (*John Arquilla*) və Devid Ronfeldt (*David Ronfeldt*) tərəfindən "Kibermüharibə gəlir!" (*Cyber War Is Coming!*) məqaləsində "Şəbəkə müharibəsi" (*Network War*) terminindən istifadə edilmişdir. Məqalədə müəlliflər kibernetik və şəbəkə müharibəsi konsepsiyalarını (*Network Centric Warfare - NCW*) irəli sürməklə müasir dövrdə İM-in təsəvvür ediləndən daha ciddi problemlər yaratmaq imkanına malik olduğunu göstərdilər [21].

Konsepsiyada İM-in əsas məqsədi kimi aşağıdakılar göstərilirdi:

1. Öz informasiyasını və informasiya sistemlərini qorumaqla qarşı tərəfin informasiya məkanına nəzarət;
2. Qarşı tərəfin informasiyasını nəzarətdə saxlamaqla informasiya hücumuna başlamaq (informasiya müharibəsi texnologiyalarından istifadə etməklə qarşı tərəfin iqtisadiyyatını ələ keçirmək və ya məhv etmək);
3. İnformasiyadan istifadə etməklə özünün ümumi güc potensialını yüksəltmək;
4. İnformasiya-psixoloji təsir vasitələrindən istifadə etməklə qarşı tərəfə psixoloji təsir göstərmək.

İnformasiya müharibəsində məqsəd və hədəflər

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:

- Məqsədin müəyyən edilməsi. "İnformasiya müharibəsi nə üçün lazımdır?" və "nəticədə nə əldə ediləcəyi gözlənilir?" suallarına cavab tapılması;
- 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;
- Taktiki fəaliyyət planının hazırlanması.

Hərbçilərin fikrincə, İM-də ilkin hədəf kimi silahlı qüvvələr, müdafiə kompleksi müəssisələri, ölkənin daxili və xarici təhlükəsizliyinə cavabdeh olan strukturlar nəzərdə tutulur. Ümumiyyətlə isə, İM-in əsas hədəfi cəmiyyətin informasiya infrastrukturudur. Hərbi analitiklərin və İKT mütəxəssislərinin gəldiyi qənaətə görə, hazırkı dövrdə İM zamanı bütün informasiya vasitələrindən və texnologiyalarından istifadə edərək, dövlətin siyasətinə qarşı narazılıq, şübhə, inamsızlıq yaradılması, ordu və əhali arasında narazılıqların artması həyata keçirilir [22].

Məqsədyönlü informasiya təsirinə məruz qalan obyektlərə uyğun olaraq informasiya hədəflərini 4 qrupa bölmək olar:

1. Qərarların qəbulu və idarəetmə sistemləri (idarə strukturları, kommunikasiya vasitələri);

2. Mülki informasiya infrastrukturu (telekommunikasiya sistemləri, nəqliyyatın, energetikanın, maliyyənin, sənayenin informasiya sistemləri);
3. Hərbi informasiya infrastrukturu (nəzarət, idarə və əlaqə sistemləri, kəşfiyyat);
4. Sosial sahələr (insanların psixologiyası, davranışları və əxlaqi stereotiplər, ayrı-ayrı şəxslər və ya sosial qruplar).

İnformasiya əməliyyatları zamanı göstərilən hədəflər müxtəlif təsirlərə məruz qala bilər. Bu yanaşma keçən əsrin 90-cı illərində daha populyar idi. Bu gün baş verən informasiya prosesləri və qarşıdurmaları sübut edir ki, informasiya sistemlərinə uzaqdan təsir müəyyən maliyyə itkilərinə və cəmiyyətdə psixoloji ab-havanın dəyişməsinə səbəb olsa da, onlar mühüm sistemlərin məhvinə və insan itkilərinə səbəb olmur. Məsələn, haker fəaliyyəti özü-özlüyündə təhlükəli olsa da, İM-də heç də həlledici rol oynamır. Odur ki, kibermüharibələrə ənənəvi hərbi əməliyyatların effektivliyini artıran faktor kimi baxmaq daha düzgündür.

Bununla belə, nəqliyyat, energetika, maliyyə və hərbi sahələrlə bağlı informasiya sistemlərinə hücum imkanlarını nəzərdən qaçırmamaq lazımdır. Bu informasiya sistemləri "kritik mühüm infrastruktur" (*critical infrastructures*) adlanan komplekslərdir. Bu hücumların mümkünlüyü iqtisadi sahədə böyük itkilərə səbəb ola bildiyinə görə, 90-cı illərin ortalarından başlayaraq kibermüharibələr hərbi və mülki ekspertlərin ciddi araşdırma predmetinə çevrilmişdir.

İnformasiya təsiri problemləri

Tədqiqatlar göstərir ki, İM texnologiyalarının araşdırılması ilə məşğul olan mütəxəssislərin işində müxtəlif yanaşmalar və baxışlar mövcud olsa da, müəyyən məsələlərdə fikirlər eynidir: İM-də əsas məqsəd qarşı tərəfi fiziki cəhətdən məhv etmək deyil, onu səhv addım atmağa sövq edərək, siyasi, hərbi, iqtisadi, psixoloji və sosial sahələrdə qələbə qazanmaq, rəqibdən üstün olmaqdır. Öz istəklərini həyata keçirmək məqsədilə mübarizə aparan tərəflər bir-birlərinin informasiya və intellektual sahələrinə təsir göstərmək üçün bütün mümkün vasitələrdən istifadə edirlər.

Müasir İM-də əməliyyatlar iki üsulla aparılır: informasiya-texniki təsir və informasiya-psixoloji təsir (cədvəl 1.).

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.

İnformasiya-psixoloji müharibə zamanı birinci yerdə ictimai fikrin formalaşdırılması prosesi dayanır. Bu halda azlıq təşkil edənlərin fikirlərini çoxluğun fikri kimi təqdim etmək informasiya-psixoloji müharibələrdə ən effektli təsir növlərindəndir. İM zamanı psixoloji müharibə vasitələrindən istifadə, bir tərəfdən, mövcud informasiya

sistemini dağıtmağa, digər tərəfdən isə, onu başqa informasiya-kommunikasiya sistemi ilə əvəz etməyə imkan verir və bununla da, cəmiyyətin maraqları ona qarşı İM aparan tərəfin maraqlarına tabe etdirilir.

Bir çox insanlar hələ də müasir İKT vasitələrindən gələn, əsasən də, siyasi məqsədlərə xidmət edən gizli informasiya-psixoloji təhlükələri tam anlamır, onlara laqeyd yanaşırlar. Müxtəlif sosial proseslərdə istifadə edilən İKT vasitələri və informasiya sistemlərinin informasiya münaqişələrində tətbiqi İM-i daha təhlükəli həddə yüksəltmişdir. İKT vasitələrinin insanlara qarşı tətbiq edilən məqsədyönlü informasiya və informasiya-psixoloji təsiri münasibətlərin sosial müxtəlifliyini təyin etməklə, daha gizli forma almaqdadır. Bu gün insan psixikasına güclü təsir edən müxtəlif, yeni mədəniyyət növləri inkişaf etməkdədir (məsələn, kompyuter mədəniyyəti, performans, qraffiti və s.).

Cədvəl 1

İnformasiya müharibəsi üsulları

İnformasiya müharibəsi	*Obyekt*	*Məqsəd*
İnformasiya-texniki təsir	Kompyuterlər və informasiya sistemləri	İnformasiya sistemlərinə nəzarət və ya onların məhv edilməsi
İnformasiya-psixoloji təsir	Ayrı-ayrı insanların şüuru və ya ictimai şüur	Hər hansı ideologiyanın təbliği və davranışların idarə edilməsi

İnformasiya müharibəsinin istiqamətləri

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 infrastruk-trunun fiziki qorunması, dezinformasiya, radioelektron mübarizə və s. daxildir. İM-in mühafizə hissəsi təhlükəsizliyin təminatı metodları ilə realizə olunur.

İM-in istiqamətlərinin çoxşaxəli olması onun xüsusiyyətinə də təsirini göstərir:

- Təsir obyekti – informasiyanın və ya informasiya sistemlərinin bütün formaları. Sərbəst obyektlər kimi bütün növ informasiya və informasiya sistemləri istifadə mühitindən ayrılmaqla təsir altında saxlanılır.
- Təsir obyekti həm silah, həm də müdafiə obyekti kimi istifadə edilir.
- Müharibə aparılan ərazi və mühit genişlənmiş olur. İM həyat fəaliyyətinin

müxtəlif sahələrində həm müharibə elan edilərkən, həm də böhran vəziyyətlərində aparılır.

- İM həm müharibə şəraitində, həm atəşkəs zamanı, həm də sülh şəraitində aparıla bilir.
- İM-də həm xüsusi təlim görmüş hərbçilər, həm də mülki şəxslər iştirak edir.

Müasir İM texnologiyalarının tətbiqində əsas strateji əsasların müəyyən edilməsi bu sahədə görüləcək ilkin məsələlərdəndir. Strateji əsasları təşkil edən məsələlər aşağıda göstərilmişdir:

- İM-in həyata keçirilməsi üçün lazım olan vasitələrə çəkilən maliyyə xərclərinin az olması;
- informasiya əməliyyatları zamanı ənənəvi dövlət sərhədlərinin maneəsiz dəf edilməsi;
- informasiya manipulyasiyası nəticəsində real vəziyyətin dərk edilməsinin idarə edilməsi;
- informasiyanın ələ keçirilməsi və saxlanması üçün strateji kəşfiyyat fəaliyyətində prioritetlərin dəyişdirilməsi;
- İM aparan tərəfin və informasiya əməliyyatlarının başlama vaxtının aşkar edilməsinin çətin olması;
- İM-ə başlayan tərəfə qarşı koalisiyanın yaradılmasının mürəkkəbliyi və s.

Bunları nəzərə alaraq, bir çox dövlətlər informasiya təhlükəsizliyini təmin etmək üçün İM-in potensialının təkmilləşdirilməsinin vacibliyinə önəm verirlər. Əgər İM-in hüçum hissəsi informasiya silahının işlənib hazırlanması və istifadəsindən asılıdırsa, müdafiə hissəsinin əsas aspekti təhlükələrin aşkar edilməsi və vaxtında qarşısının alınmasıdır.

2006-cı ildən başlayaraq ABŞ-da ölkənin görkəmli hərbi-siyasi rəhbərlərinin nümayəndələrinin iştirakı ilə "İnformasiya müharibəsi" üzrə elmi konfranslar keçirilməyə başlanmışdır. 5-ci konfrans (*5th International Conference on Information Warfare and Security*) 2010-cu ilin aprel ayında ABŞ-ın Ohayo şəhərində yerləşən Hərbi Hava Qüvvələrinin Texniki Universitetində keçirilmişdir. 6-cı konfransın 2011-ci ilin mart ayında Vaşinqton Universitetində keçirilməsi nəzərdə tutulur [24]. Konfrans materiallarını nəzərdən keçirərkən məlum olur ki, son dövrlərdə İKT mütəxəssislərini narahat edən məsələlərə, ilk növbədə, informasiya mübadiləsi şəbəkələrinə olan hücumlar, haker müharibələri, informasiya terrorizmi və kibercinayətlər aiddir.

Nəticə

Aparılan araşdırmalardan məlum olur ki, hərbi, sosial və iqtisadi sahələrdə informasiya sistemlərinin inkişafı, informasiya asılılığının güclənməsi, İM texnologiyalarının təkmilləşdirilməsi, tətbiqi və yayılması informasiya təhlükəsizliyi məsələsinin aktuallığını gündən-günə artırmaqdadır.

İKT-nin inkişafının İM-ə təsiri istiqamətlərinin analizi bir daha göstərir ki, İM zamanı informasiya texnologiyalarının məhvi, informasiyanın və informasiya sistemlərinin ələ keçirilməsi vacib məqamlardandır. Bu əməliyyatlar xüsusi qurğuların, mütəxəssislərin və proqramların köməyi ilə həyata keçirilə bilər. İM texnologiyalarının analizi nəticəsində məlum olmuşdur ki, İKT inkişaf etdikcə informasiya tədricən təminedici vasitə statusundan çıxaraq, döyüş növünə çevrilməkdədir. İqtisadi cəhətdən inkişaf etmiş ölkələrdə İKT-nin inkişaf tempinin daha da yüksək olması milli

təhlükəsizlik sistemində İM-in rolunun vacibliyini bir daha sübut edir.

Ədəbiyyat

1. Alain Decaux, Nouveaux Dossiers Secrets // Paris, SEDES, 1967, 405 pp.
2. Thomas Rona, Weapon Systems and Information War // Boeing Aerospace Co., Seattle, WA, 1976.
3. Бедрицкий А. В., Информационная война: концепции и их реализация в США // Российский институт стратегических исследований, М., 2008.
4. Martin Libicki, What is Information Warfare? //National Defense University, ACIS, 1995, pp.3.
5. Dorothy Denning, Information Warfare and Security // Addison-Wesley, 1999, p.9-19.
6. Colonel Alan D., Douglas H. Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Hardcover) // Afcea Intl Pr, 2000, pp. 309.
7. 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.
8. Molander R.C., Strategic Information warfare: A New Face of War // Washington, USA, 1996.
9. Брусницин Н.А., Информационная война и безопасность // М.: Вита-Пресс, 2001, с.9.
10. Почепцов Г.Г. Информационные войны // Киев: Ваклер, 2000. с.20.
11. Расторгуев С.П. Информационная война // М.: Радио и связь, 1998. с.35-37.
12. Цыбмал В.И. О концепции информационной войны // Информационный сборник "Безопасность". М., 1995, № 9, с.35.
13. Прохожев А.А., Турко Н.И. Основы информационной войны // Анализ систем на пороге XXI века: теория и практика. М., 1996. с.252-253.
14. Панарин И.Н. Информационные войны и Россия // Информация. Дипломатия. Психология. М.: Известия, 2002. с.145.
15. Панарин И.Н. Информационные войны: теория и практика // М.: Кадровая политика, №2, 2002.
16. Комов С.А. Информационная борьба в современной войне: вопросы теории // "Военная мысль", 1996, № 3. с.73.
17. Гриняев С.Н. Война в четвертой сфере: НВО // № 42. 2000, с.7.
18. Модестов С.А. Война, к которой готовится Америка: Эволюция вооруженной борьбы в эпоху информатизации // ЭВНГ, № 048, 1996.
19. Костин Н.А. Общие основы теории информационной борьбы // Военная мысль, №3, 1997.
20. Стрельцов А.А. Обеспечение информационной безопасности России // Теоретические и методологические основы // М.: МЦНМО, 2002.
21. Arquilla J., Ronfeldt D., Zanini M. Networks, Netwar, and Information-Age Terrorism // The Changing Role of Information in Warfare. Rand Corporation. 1999. pp.88–89.
22. Forno R., Baklarz R. The Art of Information Warfare // Insight into the Knowledge

of Warrior Philosophy, Washington, USA, 1999.
23. Швец Д.А. Информационное управление как технология обеспечения информационной безопасности // Сб. "Массовая коммуникация и массовое сознание", М., МГИМО, 2003.
24. 6th International Conference on Information Warfare and Security, The George Washington University, Washington, USA, 17-18 March 2011, http://academic-conferences.org/

УДК 004.351

Алекперова И.Я.
Институт Информационных Технологий НАНА, Баку, Азербайджан
depart17@iit.ab.az

Анализ и классификация технологий информационных войн

В статье рассматриваются причины создания технологий информационных войн, описаны проблемы, возникающие в связи с этим, а также анализируются отношение различных экспертов и ученых к термину "информационная войны". Были проанализированы классификация технологий информаци-онных войн и влияние проблемы коммуникации. Определены возможные стратегические основы в информационной войне, показаны тенденции и задачи. Проведенные исследования могут быть использованы для обеспечения информационной безопасности в сетях информационного обмена, выявления информационных угроз и выбора более эффективных средств при организации информационных контратак.

Ключевые слова: *информационная война, кибервойна, информационное оружие, информационное противостояние, компьютерное преступление, электронная война, хакер, информационно-техническое воздействие, информационно-психологическое воздействие, информационная атака.*

Alakparova I.Y.
Institute of Information Technology ANAS, Baku, Azerbaijan
depart17@iit.ab.az

Classification and analysis of information warfare technologies

In the article we observed the reasons of creation of information warfare technologies and the problems arising in this case, analyzed the relations of various experts and scientists to the term "information warfare". The classification of information warfare technologies and the influence of communication problems were. Possible strategic frameworks in information warfare were indicated, trends and targets was shown. These studies can be used to ensure information security in networks of information exchange, identify information risks and for choosing more effective means for organizing information counter.

Key words: *information warfare, cyberwar, information weapons, information counter, computer crime, electronic warfare, hacker, information-technology impact, information-psychological influence, information attack.*