UOT 2973 N 278 M

A.R. NASTAKALOV

Müdafiə Nazirliyi Rabitə və AİS idarəsi

MÜASİR ELEKTRON VASİTƏLƏRİNİN İNFORMASİYA TƏHLÜKƏSİZLİYİNƏ YARATDIĞI TƏHDİDLƏR

Məqalədə informasiya müharibəsinin tərkib hissəsi olan psixoloji müharibənin hərbi qarşıdurmalarda effektivliyinin təhlili, informasiya təhlükəsizliyinin vacibliyi və onun qorunması tədbirləri araşdırılır.

"Kim informasiyaya sahibdirsə, o da dünyaya sahibdir" ifadəsi ola bilər ki, əsasən siyasi, iqtisadi, sənaye və maliyyə baxımından söylənmişdir. Bu ifadə çox qədim dövrlərdən bu günədək dövlətlər arasında aparılan bütün növ münasibətlərdə də özünü tamami ilə doğrultmuşdur. İnformasiyanın vacibliyi dövlətlər arasındakı münasibətin bütün mərhələlərində mərkəzi yerdə olmuşdur [1].

Hərbi qarşıdurma başlayarkən informasiyanın rolu olduqca əhəmiyyətli olur. Müasir müharibələrdə qoşun növündən asılı olmayaraq hadisələrin böyük sürətlə baş verməsi tərəfləri məcbur edir ki, qarşı tərəfin niyyətini öncədən müəyyən edə bilsin və tərəflər "informasiya ovuna" başlayır. Müasir dövrdə informasiya əldə etmək üçün ayrılan vəsaitə, ixtira və tətbiq olunan kəşfiyyat vasitələrinin çeşidlərinə diqqət yetirdikdə bunun nə qədər vacib olduğunu başa düşmək çətin deyil [2].

Ölkələr müharibədən öncə və müharibənin gedişində qarşı tərəfin hərbi qulluqçuları arasında təxribat xarakterli və ya yayındırıcı məlumatların yayılması, onların ruh düşkünlüyünə nail olmaq, həmçinin, mülkü əhalidə ictimai fikrinin formalaşdırılması və yönəldilməsi məqsədi ilə onların informasiya məkanımna daxil olub aktiv informasiya fəaliyyəti göstərirlər, yəni *informasiya müharibəsi* aparırlar.

İnformasiya müharibəsi və ya qarşıdurması (ing. *InformationWar*) — informasiya sistemlərinin kənar hücumlardan müdafiəsi, eyni zamanda qarşı tərəf üzərində informasiya üstünlüyü əldə etmək məqsədi ilə həyata keçirilən informasiya əməliyyatı. Bu tip informasiya əməliyyatına qarşı tərəfə məxsus informasiya məcmusuna, informasiyaya əsaslanmış prosesləra və informasiya sistemlərinə zərər yetirməkdən ibarət fəaliyyətlər daxildir [1].

Elm və texnikanın inkişaf etdiyi hazırkı dövrdə hərbi əməliyyatlar ərəfəsində vuruşan tərəflər bir-birinin silahlı qüvvələrinin şəxsi heyətinin, həmçinin, əhalinin mənəvi-psixoloji ruhunu sarsıtmaq üçün müxtəlif vasitələrindən istifadəyə üstünlük verirlər. Bu təsir vasitələri arasında isə ən çox diqqət informasiya qarşıdurmasına ayrıldığı artıq bəzi inkişaf etmiş ölkələrin hərbi doktrinalarında da öz əksini tapmışdır.

Beləliklə, digər mübarizə metodlarından fərqli olaraq informasiya müharibələri daha geniş spektrdə aparılır və bunun həyata keçirilməsində müxtəlif vasitələrdən istifadə olunur [2].

Analitiklər informasiya mübarizələrini iki hissəyə ayırırlar:

1.İnformasiyadan müdafiə - öz məlumatların və informasiya strukturlarının düşmən təsirindən müdafiəsidir;

2.İnformasiya zərbəsi – düşmənin informasiya infrastrukturunun tam məhv edilməsi və düşmənə öz qüvvəsindən istifadə imkanından məhrum etməkdən ibarətdir.

Qeyd edək ki, hazırkı dövrdə internet vasitəsi ilə düşmənin həyati əhəmiyyətli maliyyə, bank sistemi, rabitə, elektrik təchizatı və nəqliyyat vasitələrini iflic etmək mümkündür [1-3].

İnformasiya dağıdıcı xarakter daşıyır və bütövlükdə döyüşən strukturları, iqtisadi və sosial sistemləri sıradan çıxarır. İnformasiya mübarizələrinin əsas özünəməxsusluğu isə ondan ibarətdir ki,

tərəflər öz informasiya üstünlüyünü lazımi səviyyədə qoruyub saxlamaqla düşmənin informasiya sistemini dağıtmağa çalışırlar [4].

Psixoloji müharibə (psixoloji əməliyyat və ya xüsusi təbliğ) – düşmən qoşunlarının (qüvvələrinin) mənəvi düşkünlüyünə (demoralizə) və qarşıdurmadan yayınmasına nail olmaq məqsədi ilə aparılan psixoloji təsirdir. O, döyüş əməliyyatlarının hazırlıq mərhələsində və ya əməliyyat zamanı aparıla bilər [5].

Hərbi məqsədlər üçün tətbiq olunan ilk dezinformasiya nümunələri XIII əsrə təsadüf edir. Burada düşmən qoşun rəhbərlərinə öz krallarının adından yalan əmrlər çatdırılır və döyüş fəaliyyətini dayandırmağa məcbur edilir.

Psixoloji təsirlə bağlı işlər, həmçinin, öz qoşunlarının hərbi qulluqçuları arasında da aparılırdı. Belə ki, düşmənə əsir düşməkdən çəkindirmək üçün düşmənin amansız olduğu, heç kimə rəhm etmədiyi və yalnız zülm vermək üçün bəzilərini sağ saxladığı vurğulanırdı. Qarşı tərəf isə, əksinə bəzi əsirlərlə yaxşı davranaraq onları geri buraxırdı ki, digər əsgərlərdə də sağ qalmaq üçün əsirə düşmə fikri oyansın.

Birinci dünya müharibəsində psixoloji müharibənin əsas formaları vərəqələr, kitabçalar, açıqcalar, plakatlar və yalançı ərzaq talonları olmuşdur.

Birinci dünya müharibəsi bitən kimi qərb ölkələrində psixoloji müharibə məsələlərini əks etdirən onlarla tədqiqat işi yazıldı, bir çox universitetlərdə ixtisaslaşmış mütəxəssislər yetişdirən kafedralar yarandı.

İkinci dünya müharibəsində yuxarıda qeyd olunan üsullardan fərqli olaraq artıq yalançı radioyayımlardan da istifadə etməyə başlandı [6].

İkinci dünya müharibəsində, həmçinin, vəzifəli şəxslərə qarşı şübhə oyandıraraq qarşı tərəfin şəxsi heyətini demorəlizə etmə cəhdləri həyata keçirilirdi.

Müttəfiqlərin psixoloji müharibəsinin effektivliyini isbat edən faktlardan biri də odur ki, 1943-cü ildə Tunis hücum əməliyyatı zamanı Amerikanın əsrliyinə icazə-vərəqəsini əldə etmək üçün İtaliya əsgərləri bir-birindən ona 600 frank verməyə hazır idilər. Bu fakt bir çox Amerika hərbi rəhbərliyin psixoloji müharibə metodları haqqında öz skeptik fikrini dəyişməyə məcbur etdi.

Qarabağ müharibəsində düşmənlərimiz məhs yuxarıda qeyd olunan metodlardan aktiv istifadə edirdilər. Onlar müharibənin əvvəlində əsr düşən əsgərlərimizə yalnız qarabağlılarla vuruşduqlarını və Azərbaycanın digər rayon və şəhər əhalisi ilə heç bir işlərinin olmadığını inandırmağa çalışırdı. Əsrlikdən qayıdanlardan bəziləri qeyd olunan psixoloji təsir altında yerlərdə başa düşmədən həmin təbliğatı aparırdılar. Sonralar isə əksinə işğal etdikləri rayon və kənd əhalisinə qarşı misli görünməyən vəhşilik göstərməklə digər ətraf rayon və kənd əhalisində də qorxu və düşmənin qarşısında durmağın mümkünsüz olduğu hissi yaradıldı, həmçinin, əhalidə xüsusi casuslar vasitəsi ilə, ölkənin siyasi və hərbi rəhbərliyinə qarşı inamsızlıq, bacarıqsızlıq və çarəsizlik hissləri yaradılırdı. Bunun nəticəsində demoralizə olunmuş əhalimizin müqavimət göstərmə iradəsi sarsıldı və böyük torpaq itkilərinə məruz qaldıq.

2016-cı ilin Aprel döyüşlərində əldə etdiyimiz hərbi üstünlüyümüz əhalimizdə böyük ruh yüksəlişinin yaranmasına səbəb oldu. Bunu görən mənfur düşmənimiz döyüş meydanında itkilərini gizlətmək üçün kütləvi informasiya vasitəsi ilə onların az itki verdiyini, bizim tərəfin isə əksinə dəfələrlə çox itki verdiyini hər iki tərəfə çatdırmağa çalışırdılar. Hətta, İnternet resurslarında guya Azərbaycan Ordusunun hərbi rəhbərliyinə aid və bunu təsdiqləyən yalançı raport-məruzə nümunələri yerləşdirmişdilər.

Yuxarıda qeyd olunan misallardan açıq-aydın görünür ki, yaxşı düşünülmüş və dəqiq yerinə yetirilmiş informasiya zərbəsi və müdafiəsi minimal fiziki güc tətbiq etməklə qarşı tərəfin döyüş qabiliyyətini əhəmiyyətli dərəcədə sarsıtmaq mümkündür [7].

Müasir zamanda da düşmənə psixoloji təsir etmək üçün ənənəvi metodlarla yanaşı internet şəbəkəsindən geniş istifadə edirlər. Onlar müxtəlif sosial saytlara daxil olur, yaxınları ilə yazışır, müxtəlif forumlarda müzakirələrə qoşulur, xəbərlər verilişlərini izləyir, musiqi çarxları və kinoları seyr edir. Habelə müxtəlif internet resurslarından istifadə edərək bir-biri ilə məlumat, foto və video mübadiləsi həyata keçirirlər.

Bütün bunları nəzərə aldıqda aydın olur ki, əhalimizin və ələlxüsus gənclərimizin (hərbi qulluqçuların) informasiya müharibəsinin hədəfinə və psixoloji təsirin qurbanına çevirməyə yönəlmiş məqsədyönlü işlər aparılmaqdadır.

Bəzi ölkələrin xüsusi xidmət orqanları virusların və casus proqramlarının yüklənməsi üçün kompüterlərə və yaddaş qurğularına müdaxilə etmə imkanını, bu vasitələrin satışa çıxardılmasından öncə əldə edirlər. Qeyd olunan vasitələr sərfəli qiymətlərlə bazarda təklif olunur, üstəlik sərgilərdə və ya digər tədbirlərdə iştirakçılara hədiyyə və ya suvenir kimi verilə bilər. Bəzən virusa yoluxdurulmuş yaddaş qurğuları xüsusi orqanların marağında olan şəxslərin nəzərini cəlb edən yerlərdə qəstdən yerləşdirilir.

Dünyada antivirus proqramları istehsal edən bir çox şirkətlər mövcuddur, lakin onların əksəriyyəti öz ölkələrinin xüsusi xidmət orqanları ilə əməkdaşlıq edir. Bu proqramlardan istifadə edən hər bir kompüterə və ya mobil elektron vasitəsinə müdaxilə etmə imkanı yaranır. Belə ki, onlarda yerləşən, gələn və ya çıxan məlumatlar düşmən tərəfindən əldə edilə və təhrif edilə bilər, üstəlik onların sahiblərinin koordinatlarının təyin olunması mümkündür [7].

Əməliyyat sistemlərinin lisenziyalı olması informasiya təhlükəsizliyi baxımından çox vacib amildir. Təəssüf ki, əksər istifadəçilər onların pirat versiyalarını istifadə etdiyinə görə bu imkandan istifadə edə bilmirlər və hackerlər bu boşluqdan istifadə edə bilirlər.

Hal-hazırda konflikt tərəflərinin informasiya qarşıdurması maraqlarında internetdən daha aktiv və genişmiqyaslı tətbiq olunur. Buna səbəb internetin digər vasitələrə nisbətən operativliyi, iqtisadi cəhətdən daha səmərəliyi, təsir mənbəyinin gizliliyi, kompüter sistemlərinə məsafəsən təsiri, mümkün olan nəticələrin miqyası, məlumatın eyni zamanda böyük kütləyə çatdırılması kimi üstünlüklərinin olmasıdır [7].

Beləliklə, informasiya təhlükəsizliyinin təmin edilməsi və psixoloji təsirləri azaltmaq məqsədi ilə aşağıdakı tədbirlərin həyata keçirilməsi təklif olunur [8-10]:

1.Xidməti kompüterlərin, yaddaş qurğularının və digər elektron vasitələrin təhlükəsiz istismarı barədə rəhbər edici təlimatların tələblərinə ciddi riayət edilməsinə nail olunması;

2.Kompüterlərdə istifadəyə icazəsi olan hər bir istifadəçi üçün ona məxsus qeydiyyat adının (login) və parolun yaradılması, inzibatçı (administrator) hüquqi yalnız səlahiyyətli şəxslərdə olmalı, hətta onların belə gərəksiz hallarda bu hüquqdan istifadə etməsi;

3.Lokal şəbəkələrdə kompüterlərə məlumatın daxil edilməsi və ya çıxardılması yalnız müvafiq qaydada vahid mərkəzdən təşkil olunması və qeydiyyatı aparılması;

4.Kompüterdə olan proqram təminatları, ələlxüsus əməliyyat sistemi və antivirus proqramları lisenziyalı olması və mütəmadi olaraq yenilənməsi;

5.İT mütəxəssisləri tərəfindən hərbi hissənin kompüterlərinin mütəmadi təftişi və yeni yaranan təhdidlər haqqında istifadəçilərin daimi maarifləndirməsi;

6.Şəxsi heyətin asudə vaxtlarını maraqlı keçirmək üçün təşkil olunan müxtəlif əyləncə proqramları çərçivəsində maarifləndirici, vətənpərvərlik hislərini artıran, həmçinin, topoqrafik xəritələr, müxtəlif silahlar və hərbi texnikalar istifadə olunan hərbi yönlü kompüter oyunlarının təşkili;

7.Cəbhəyanı rayonların mülki əhalisi ilə işlərin təşkili, onların informasiya təhlükəsizliyi baxımından maarifləndirilməsi və ayıq-sayıqlığını artırması məqsədi ilə yerli hüquq mühafizə orqanlarının və bələdiyyə idarəsinin əməkdaşları ilə əməkdaşlığın mütəmadi olaraq təşkili;

8.Hərbi qulluqçuların şəxsi elektron vasitələrinin MAC adreslərini təyin edilməsi, internetə çıxışını və onlarla ünsiyyət qurmağa çalışanları nəzarətdə saxlanılması, onları internetdə ehtiyatsız davranışlardan çəkindirmək üçün profilaktik tədbirlər görülməsi, həmçinin, onlara qarşı həyata keçirilən kiber hücumların qarşısını almaqda onlara kömək edilməsi;

9.İnsanların maraq kəsb etdiyi saytların özümüzə məxsus prototiplərinin yaradılması və əsl sayta sorğu həyata keçirildikdə bu saytlara yönləndirilməsinin təşkili;

10.Kiber müdafiə ilə məşğul olan mütəxəssislər İnternet məkanını daimi izləməli, bizim saytlar kimi təqdim olunan düşmənə məxsus saytları aşkar etməli və onların bağlanması üçün tədbirlər görməlidir;

11.Xidməti istifadə üçün tətbiq olunan yaddaş qurğuları yalnız etibarlı mənbələrdən mərkəzləşdirilmiş şəkildə əldə olunması, onların ID kodları qeydiyyata götürülməli və viruslara yoluxmasının qarşısını almaq məqsədi ilə İT mütəxəssisləri tərəfindən mütəmadi olaraq yoxlanılması, hərbi qulluqçuların şəxsən əldə etdikləri yaddaş qurğularının qeydiyyatdan keçirilməsi və qeydiyyatdan keçmədikdə isə istifadəyə buraxılmasına qadağanın qoyulması;

12.Hərbi qulluqçuların ayıq-sayıqlığını artırmaq üçün müxtəlif üsullardan istifadə edərək onların informasiya təhlükəsizliyi baxımından sınanması və nəticələrin digər hərbi qulluqçulara çatdırılması.

NƏTİCƏLƏR

1.Müasir müharibələrdə informasiya amili həyatı vacib rol oynayır.

2.İnformasiya vasitəsi ilə dövlətlər arasında yaranan konflikt vəziyyəti müharibəyə çevrilmədən həllinə nail olmaq mümkündür.

3.İnformasiya vasitəsi ilə müharibədən öncə, müharibə zamanı və müharibədən sonra öz tərəfinə müttəfiqləri cəlb edib ittifaq yaradmaq olar.

4.İnformasiya vasitəsi ilə dünya və ölkə ictimaiyyətini aparılan müharibənin ədalətli olduğuna inandırmağa, qarşı tərəfin digər ölkələr tərəfindən dəstəklənməsinin qarşısını almağa, informasiya cəhətdən təcrid etməsinə, müharibənin nəticələrini bütün dünya ölkələri tərəfindən tanımasına və sülh müqaviləsinin öz xeyrinə bağlanmasına nail olmaq mümkündür.

5.İnformasiya sahəsinə zəifliklər, təhdidlər və risklər günbə-gün artdığına görə kiber təhlükəsizlik sahədə işlər davamlı və kompleks şəkildə aparılmalıdır.

6.Əhalinin informasiya təhlükəsizliyi haqqında maarifləmə işlərinin məktəb dövründən başlayaraq bütün mərhələlərdə aparılmalıdır.

ƏDƏBİYYAT

1.Daniel Ventre, "Cyberwar and Information Warfare", Wiley – ISTE, 2011,448 p.

2.EdwardWaltz, "InformationWarfarePrinciples and Operations",ArtechHouse, 1998, 397 p.

3.Шустов В. Войны и сражения Древнего мира. Ростов-на-Дону: «Феникс», 2006. 521 с.

4.Рогозин Д. Война и мир в терминах и определениях. Военно-технический словарь. Издательство "Вече", 2016. 272 с.

5.Психологическая война. Приемы психологической войны, psywar41.htm, Accesstime 2001.

6.Greco-PersianWars, https://www.britannica.com/event/Greco-Persian-Wars,Access time 2017

7.Управление доступом критическим ресурсам, https://www.anti-malware.ru /threats/ information-security-threats/, Access time 2017.

8.Gregory J. Touhill, C. JosephTouhill Cybersecurityfor Executives, the American Institute of Chemical Engineers, Inc, 2014.

9.M. Morgan, Cisco CCNA SecurityNotes, the USA, 2010.

10.M. Morgan, Cisco IOS LAN SwitchingCommandReference, San Jose, Americas Headquarters, 2010.