Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 106-115
MİLLİ TƏHLÜKƏSİZLİK ***NATIONAL SECURITY***

UOT 355/359 DOI: 10.30546/9878.2024.2.10.0032.

İNFORMASİYA MÜHARİBƏSİ VƏ MİLLİ TƏHLÜKƏSİZLİK

polkovnik-leytenant Rəşadət Orucov
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
orujovrashadat@gmail.com

Xülasə. Məqalədə informasiya müharibəsinin milli təhlükəsizlikdə rolu və milli təhlükəsizliyə təsiri, informasiya müharibəsinə konseptual baxış, eləcə də informasiya müharibəsinə qarşı mübarizə strategiya nümunələri öz əksini tapır. Münaqişələrdə üstünlük əldə etmək və ya strateji məqsədlərə nail olmaq üçün informasiya və kommunikasiya texnologiyalarından istifadənin əhəmiyyəti, strateji kommunikasiya sistemlərinin fəaliyyətinə və nəticələrə mənfi təsir göstərmək üçün məlumatın manipulyasiyası, istismarı və yayılması kimi məsələlərə toxunulur. O cümlədən informasiya üstünlüyü uğrunda mübarizənin milli təhlükəsizlik kontekstində həlledici rol oynadığı izah edilir. Tədqiqatın məqsədi vətəndaşlar arasında media və rəqəmsal savadlılığı və tənqidi düşüncənin artırılması, fərdlərdə yanlış məlumatı müəyyən və ayırd etmək bacarığının formalaşdırılmasıdır. Bu çərçivədə təhsil proqramları fərdlərə mənbələri qiymətləndirməyə, məlumatı və faktları yoxlamağa, məzmunu tənqidi təhlil etməyi öyrənməyə imkan verir. Məqalədə həmçinin dövlətlərin və beynəlxalq təşkilatların informasiya müharibəsi ilə kollektiv mübarizədə normalar, qanunlar və vahid çərçivələrin yaradılması üçün kəşfiyyat məlumatlarının mübadiləsi, kiberhücumlara cavab tədbirlərinin əlaqələndirilməsi və informasiya məkanında məsuliyyətli davranışın təşviqi sahəsində əməkdaşlığından bəhs edilir.

Açar sözlər: strateji kommunikasiya, milli təhlükəsizlik, informasiya müharibəsi, kommunikasiya texnologiyaları, məlumat mübadiləsi

Giriş

Son illər informasiya müharibəsinin milli təhlükəsizliyin təmin olunması istiqamətində ciddi problemlərə gətirib çıxardığının şahidi oluruq. Müasir rəqəmsal əsrdə məlumatın manipulyasiyası və mənfi yönümlü istifadəsi xalqların sabitliyi və təhlükəsizliyinə əhəmiyyətli dərəcədə təsir göstərmə gücünə malikdir. Bu məqalə informasiya müharibəsi anlayışını və onun milli təhlükəsizliyə təsirini işıqlandırmaq məqsədi daşıyır. Məqalədə, həmçinin informasiya müharibəsinə qarşı mübarizə strategiyaları araşdırılır və onun təzahürlərini əks etdirən real dünya nümunələri öz əksini tapır.

İnformasiya müharibəsi münaqişələrdə üstünlük əldə etmək və ya strateji məqsədlərə nail olmaq üçün informasiya və kommunikasiya texnologiyalarından istifadə edən bir sıra fəaliyyətləri əhatə edir. O, qavrayışları formalaşdırmaq, strateji kommunikasiya sistemlərinin fəaliyyətinə mənfi təsir göstərmək və nəticələrə təsir etmək üçün məlumatın manipulyasiyası, istismarı və yayılmasını ehtiva edir. Dünyada baş verən hadisələr fonunda informasiya üstünlüyü uğrunda mübarizə milli təhlükəsizlik kontekstində həlledici rol oynayır.

İnformasiya müharibəsinin milli təhlükəsizliyə təsiri geniş və çoxşaxəlidir. O, siyasi fəaliyyətlərə və demokratik proseslərə informasiya sisteminin boşluqlarından istifadə edilməklə mənfi təsir göstərə bilər. İctimai rəyin manipulyasiyası, yalan məlumatların yayılması və dövlət qurumlarına inamın azalmasını informasiya müharibəsinin nəticəsi hesab etmək olar. İnformasiya müharibəsinə qarşı mübarizə və milli təhlükəsizlik maraqlarının qorunması ilə bağlı effektiv strategiyaların hazırlanması üçün bu təsirləri dərk etmək və onların həlli yollarını müəyyənləşdirmək zəruridir.

İnformasiya müharibəsinə qarşı mübarizə fəal tədbirləri, müdafiə mexanizmlərini və birgə səyləri özündə birləşdirən hərtərəfli yanaşmanı əks etdirməlidir. İnformasiya müharibəsinə qarşı mübarizə strategiyalarına kritik infrastrukturun qorunması üçün kibertəhlükəsizlik tədbirlərinin gücləndirilməsi, fərdlərin media savadlılığının və rəqəmsal vətəndaşlıq təhsilinin təşviqi, norma və çərçivələrin yaradılmasında beynəlxalq əməkdaşlığa sövq edilməsi, effektiv əks-təbliğat və strateji kommunikasiyanın inkişaf etdirilməsi daxildir. Bu strategiyalar informasiya müharibəsinin risk və

təsirlərini azaltmaq, milli təhlükəsizlik maraqlarını və informasiya ekosisteminin bütövlüyünü qorumaq məqsədini daşıyır.

Qeyd etmək lazımdır ki, dünyada baş vermiş hadisələr fonunda informasiya müharibəsində tətbiq edilən taktikaların və xalqların üzləşdiyi nəticələrə dair konkret nümunələrin öyrənilməsi mühümdür. Belə ki, Rusiyanın 2016-cı il ABŞ prezident seçkilərinə müdaxiləsi, kritik infrastruktura kiberhücumlar, İraq–Şam İslam Dövlətinin (İŞİD) təbliğatı və terror təşkilatına cəlbetmə, seçkilərdə dezinformasiya kampaniyaları kimi bariz nümunələr informasiya müharibəsinin müxtəlif təzahürlərini nümayiş etdirir. Bu nümunələri araşdırmaqla siyasətçilər, təhlükəsizlik mütəxəssisləri və tədqiqatçılar informasiya müharibəsi ilə mübarizədə mürəkkəb vəziyyəti və yaranan problemlərin həlli yollarını tapmağa kömək edə bilər.

Nəticə etibarilə, informasiya müharibəsi qloballaşan dünyada milli təhlükəsizliyə ciddi problemlər yaradır. Onun konseptual əsaslarını dərk etmək, təsirini qiymətləndirmək, onunla mübarizə aparmaq üçün effektiv strategiyaların işlənib hazırlanması və bu istiqamətdə dünyada baş vermiş hadisələrin araşdırılması milli təhlükəsizlik maraqlarının qorunmasında mühüm əhəmiyyət kəsb edir. Dövlət və ona bağlı qurumlar informasiya müharibəsinin manipulyativ və istismarçı aspektlərini aradan qaldırmaqla, proaktiv tədbirlər hazırlaya, kibertəhlükəsizliyi inkişaf etdirə, media savadlılığını təşviq edə, beynəlxalq əməkdaşlığı inkişaf etdirə və milli təhlükəsizliyin qorunması və informasiya ekosistemlərinin bütövlüyünün qorunması məqsədilə effektiv əks-tədbirlər həyata keçirə bilər.

İnformasiya müharibəsinə konseptual baxış

İnformasiya müharibəsi milli təhlükəsizliyi formalaşdıran müasir münaqişələrin mühüm aspekti kimi meydana gəlmişdir. Texnoloji tərəqqi və qarşılıqlı əlaqə ilə müəyyən edilən bir dövrdə informasiya üstünlüyü uğrunda mübarizə həlledici xarakter almışdır. Bu bölmədə informasiya müharibəsinə konseptual baxış, onun təbiəti, məqsədləri, dövlət və qeyri-dövlət subyektləri tərəfindən istifadə olunan strategiyalar araşdırılır.

İnformasiya müharibəsi münaqişələrdə üstünlük əldə etmək və ya strateji məqsədlərə nail olmaq üçün informasiya və kommunikasiya texnologiyalarından istifadəni ehtiva edir. O, qavrayışlara təsir etmək, kommunikasiya sistemlərinin fəaliyyətinə zərər vurmaq və nəticələri formalaşdırmaq üçün məlumatın manipulyasiyası, istismarı və yayılmasını əhatə edir. İnformasiya müharibəsindən qarşı tərəfi aldatma, inandırma və ya pozucu fəaliyyət vasitəsi kimi istifadə edilir. Bundan əlavə, informasiya müharibəsi taktiki, əməliyyat və ya strateji məqsədlərə nail olmaq üçün informasiyanın və onunla əlaqəli texnologiyaların istifadəsi kimi də qəbul edilə bilər. Bu, kiberhücumlar, psixoloji əməliyyatlar, təbliğatın yayılması, dezinformasiya kampaniyaları və sosial mühəndislik daxil olmaqla, geniş fəaliyyət spektrini əhatə edir [1].

İnformasiya müharibəsi cəlb olunan aktorların motivasiya və niyyətindən asılı olaraq, bir sıra məqsədlərə xidmət edir. Bu məqsədlərə aşağıdakılar aid edilə bilər:

– təsir və inandırma. İnformasiya müharibəsi təbliğat, dezinformasiya və ya məlumatların məqsədli yayılması yolu ilə ictimai rəyi formalaşdırmaq, qərar qəbuletmə proseslərinə təsir etmək və qavrayışları dəyişdirmək məqsədini daşıyır. Aktorlar ictimai əhval-ruhiyyəyə təsir etməklə, öz məqsədlərinə dəstək əldə etməyə, düşmənləri gözdən salmağa və ya öz hərəkətlərinə haqq qazandırmağa çalışırlar;

– təhlükə və inkar. İnformasiya müharibəsi informasiya sistemləri, şəbəkələri və ya kritik infrastrukturun fəaliyyətinə zərər vurmaq və ya onu məhdudlaşdırmaq üçün istifadə edilə bilər. Kiberhücumlar, informasiya manipulyasiyası və ya yalan məlumatların yayılması məlumatın bütövlüyünü pozmaq, onun etibarlılığına zərər vurmaq və çaşqınlıq yaratmaq, xaosla və ya dövlət qurumlarına inamın itirilməsi ilə nəticələnə bilər;

– casusluq və kəşfiyyat məlumatlarının toplanması. İnformasiya müharibəsi kibercasusluq, müşahidə və ya sosial mühəndislik vasitəsilə həssas və ya məxfi məlumatların toplanmasını əhatə edə bilər. Bu məlumatlar strateji üstünlük, kəşfiyyat məqsədləri və ya rəqiblərin imkanları və niyyətləri barədə məlumat toplamaq məqsədilə istifadə edilə bilər [2];

– psixoloji əməliyyatlar. Əhalinin rəftarı, inancı və davranışlarına təsir etmək məqsədini daşıyır. Təbliğat, aldatma və ya qavrayış idarəçiliyi kimi taktikalardan istifadə etməklə, informasiya müharibəsi çaşqınlıq yaradır, düşmənləri ruhdan salır və ya əməliyyatları həyata keçirən aktorun maraqlarına üstünlük vermək üçün rəy formalaşdırır [3].

İnformasiya müharibəsi informasiya sistemləri və şəbəkələrindəki boşluqlardan istifadə etməklə, bir çox yanaşmaları özündə əks etdirir. Bəzi ümumi yanaşmaları aşağıdakı kimi qruplaşdırmaq olar:

– kiberhücumlar – məlumat sistemlərini, şəbəkələri və ya kritik infrastrukturun fəaliyyətini dayandırmaq və ya məhdudlaşdırmaq üçün zərərli proqramların, hakerlərin və ya xidmətdən imtina hücumlarının (DDOS) istifadəsini əhatə edir. Kiberhücumçular (hakerlər) icazəsiz giriş əldə etmək, məlumatları oğurlamaq, əməliyyatları məhdudlaşdırmaq və ya ziyan vurmaq üçün texnologiyanın zəif tərəflərindən istifadə edir [4].

– dezinformasiya və təbliğat. Dezinformasiya kampaniyaları hədəf auditoriyasını aldatmaq üçün bilərəkdən yalan və ya yanlış məlumat yaymaq məqsədini daşıyır. Burada təbliğat qavrayışlarını formalaşdırmaq, ictimai rəyi manipulyasiya etmək və ya müəyyən səbəb və ya ideologiyaya dəstək vermək üçün qərəzli, yaxud seçmə məlumatların yayılması nəzərdə tutulur.

– sosial mühəndislik. Bu taktika etibardan sui-istifadə etmək, həssas məlumatları oğurlamaq, sistemlərə və ya şəbəkələrə icazəsiz giriş əldə etmək üçün insan psixologiyasının manipulyasiyasını nəzərdə tutur. Fiziki və hüquqi şəxsləri aldatmaq məqsədilə, adətən, "fişinq" kimi üsuldan istifadə edilir [5].

– qavrayışın idarə edilməsi – ictimai rəyə təsir etmək üçün məlumatların və rəylərin formalaşdırılmasını və məlumat axınına nəzarəti əhatə edir. Media manipulyasiyası, strateji mesajlaşma və ya rəylərin idarə edilməsi, eyni zamanda məlumatın yayılmasını istiqamətləndirmək üçün sosial media platformalarından istifadə etməklə həyata keçirilə bilər [6].

İnformasiya müharibəsi təsir və çətinlikləri özündə ehtiva edir. Bu təsir və çətinliklərə aşağıdakılar şamil edilə bilər:

– sürətli texnoloji tərəqqi. Texnologiyanın daim inkişaf edən təbiəti potensial təhlükələri qabaqlamaqda bir çox çətinliklər yaradır. İnformasiya müharibəsi ilə məşğul olan aktorlar davamlı olaraq, ayıq-sayıq olmalı və yeni texnologiyalardan istifadə etməklə, onları öz fəaliyyət tərzlərinə uyğunlaşdırmalıdır;

– sahələrarası təsir. İnformasiya müharibəsi siyasi, iqtisadi və sosial sahələrdə fəaliyyət göstərir. O, ənənəvi hərbi arenalardan kənara çıxaraq ictimai rəy, iqtisadi sabitlik, sosial birlik və siyasi proseslərə təsir edə bilər. Bu sahələrarası təsirləri qavramaq və problemləri həll etmək milli təhlükəsizlik istiqamətində cavab tədbirləri üçün vacibdir;

– tanınma problemləri. İnformasiya müharibəsi fəaliyyətinin mənbəyini müəyyən etmək mühüm problemdir. Çətin aktorlar tez-tez gizli şəkildə "bot" şəbəkələrindən istifadə edir və ya müəyyən dərəcədə anonimliyi təmin edən vasitələrlə öz həqiqi şəxsiyyətini maskalamaq üçün bir çox yanaşmalardan istifadə edir. Bu isə hücumların dəqiq mənbəyini müəyyən etməyi və onlara qarşı müvafiq cavab tədbirlərini çətinləşdirir;

– inkişaf etməkdə olan tənzimləyici çərçivələr. İnformasiya müharibəsinin sürətlə artması möhkəm hüquqi və tənzimləyici çərçivələrin işlənib hazırlanmasını tələb edir. Kiberməkanı idarə etmək, informasiya texnologiyalarından yanlış məqsədlər üçün istifadə olunması ilə mübarizə məqsədilə norma, qayda və protokolların yaradılmasında beynəlxalq əməkdaşlıq həyati əhəmiyyət kəsb edir. İnformasiya müharibəsinin inkişaf edən təbiəti hüquqi bazaların təkmilləşdirilməsi və gücləndirilməsi üçün davamlı olaraq, səylər tələb edir [7].

Yuxarıda qeyd edilən məqamlara əsasən milli təhlükəsizlik kontekstində informasiya müharibəsinin mürəkkəb və çoxşaxəli sahədə yayılmasını qeyd etmək olar. Onun konseptual əsaslarını anlamaq effektiv cavab tədbirlərinin görülməsində və müdafiə fəaliyyətlərinin həyata keçirməsində önəmlidir. Göründüyü kimi, informasiya texnologiyaları inkişaf etdikcə informasiya müharibəsində istifadə olunan taktika və strategiyalar da inkişaf edəcəkdir. İnformasiya müharibəsinin məqsədlərini, strategiyalarını və nəticələrini dərk etməklə, dövlət və ona bağlı olan qurumlar, o cümlədən təşkilatlar

milli təhlükəsizlik maraqlarını qorumaq üçün fəal tədbirlər hazırlaya bilər. Əməkdaşlıq, texnoloji tərəqqi, beynəlxalq əməkdaşlıq və möhkəm hüquqi bazaların inkişafı informasiya müharibəsinə qarşı mübarizədə, eləcə də rəqəmsal əsrdə dövlətin təhlükəsizliyi və sabitliyinin təmin edilməsi üçün vacibdir.

İnformasiya müharibəsinin milli təhlükəsizliyə təsiri

Rəqəmsal əsrdə informasiya müharibəsi milli təhlükəsizlik üçün əhəmiyyətli problem kimi ortaya çıxmışdır. Qloballaşan dünyada informasiya üstünlüyü uğrunda mübarizə dövlətlərin təhlükəsizliyi və sabitliyi üçün vacib amildir. Bu məqalə informasiya müharibəsinin milli təhlükəsizlik fonunda siyasi, iqtisadi, sosial və digər sahələrə təsirlərini tədqiq edir.

Siyasi təsir. İnformasiya müharibəsi güc, idarəetmə və beynəlxalq münasibətlərin dinamikasına təsir edə bilir. Bu təsirlərə aiddir:

– seçkilərə müdaxilə. Rəqib aktorlar seçki proseslərinə müdaxilə etmək üçün informasiya müharibəsi taktikalarından məharətlə istifadə edir. Onlar dezinformasiya yaymaq, kiberhücumlar həyata keçirmək və ya ictimaiyyətə təsir kampaniyaları vasitəsilə ictimai rəyi formalaşdırmaq, demokratik proseslərə inamı sarsıtmaq və seçkilərin nəticələrini manipulyasiya etmək kimi fəaliyyətləri həyata keçirir;

– dövlətin sabitliyinin pozulması. İnformasiya müharibəsi nifaq salmaq, sosial iğtişaşları qızışdırmaq və ya ictimai etimadı pozmaq kimi fəaliyyətlərlə dövlətin sabitliyinə xələl gətirə bilər. Məlumatların manipulyasiyası mövcud ictimai parçalanmalardan istifadə edə, dövlətin legitimliyini zəiflədə və siyasi qarışıqlıq yarada bilər;

– siyasi proseslərə təsir. İnformasiya müharibəsi siyasi proseslərə təsir göstərə bilər. Aktorlar ictimai rəyi manipulyasiya etməklə gündəmi formalaşdıra, siyasi qərarları idarə edə və effektiv idarəçiliyə mane ola bilər. Yanlış məlumat və təbliğat kampaniyaları ictimai əhval-ruhiyyəni dəyişdirə, yanlış qərarların qəbul edilməsinə səbəb ola bilər [8].

İqtisadi təsir. İnformasiya müharibəsi sənaye, maliyyə sistemləri və iqtisadi sabitliyə təsir edən iqtisadi problemlər yaradır. Bu təsirlərə aşağıdakılar aid edilə bilər:

– kritik infrastruktura qarşı fəaliyyətlər. Elektrik şəbəkələri, nəqliyyat sistemləri və ya kommunikasiya şəbəkələri kimi kritik infrastrukturu hədəfə alan kiberhücumlar iqtisadi təsirlərə səbəb ola bilər. Potensial nəticələrə maliyyə itkilərini və ictimai təhlükəsizliyin pozulmasını aid etmək olar;

– əqli mülkiyyət oğurluğu. İnformasiya müharibəsi əqli mülkiyyət oğurluğuna, innovasiyalara və iqtisadi rəqabət qabiliyyətinə təhlükə yarada bilər. Dövlət tərəfindən maliyyələşdirilən aktorlar və ya kibercinayətkarlar əqli mülkiyyətə, ticarət, tədqiqat və sənaye sirlərinə, həmçinin inkişafedici məlumatlara icazəsiz giriş əldə etmək üçün biznesləri, tədqiqat institutlarını və ya dövlət qurumlarını hədəfə alır [9];

– maliyyə bazarının manipulyasiyası. Yanlış məlumatların yayılması və ya maliyyə sistemlərinə koordinasiyalı şəkildə hücumların həyata keçirilməsi kimi informasiya müharibəsi taktikaları bazar sabitliyini və investorların inamını sarsıda, dəyişkənlik, iqtisadi itki və maliyyə institutlarına olan inamın azalmasına səbəb ola bilər [10; 90].

Sosial təsir. İnformasiya müharibəsi ictimai əhval-ruhiyyəyə, cəmiyyətin birliyi və fərdi davranışa təsir edən əhəmiyyətli sosial təsirlərə malikdir. Müəyyən əsas təsirlərə aşağıdakılar daxildir:

– ictimai rəyin manipulyasiyası. İnformasiya müharibəsi dezinformasiya, təbliğat yaymaq və ya məlumatlara təsir etməklə ictimai rəyi manipulyasiya edə bilər. Bu, cəmiyyətlərin qütbləşməsinə, sosial bölünmələrin artmasına, institutlara və mediaya olan inamın azalmasına səbəb ola bilər;

– sosial media platformalarının istismarı. Sosial media platformaları informasiya müharibəsi fəaliyyətləri üçün əlverişli şəraitə çevrilmişdir. Rəqib aktorlar bu platformalardan yanlış məlumat yaymaq, ictimai müzakirələri manipulyasiya etmək və mövcud ictimai disbalansın pozulmasını artırmaq məqsədilə istifadə edir ki, bu da cəmiyyətdə iğtişaşlara və gərginliyə gətirib çıxarır;

– məxfilik və şəxsi təhlükəsizliyə təhdidlər. İnformasiya müharibəsi şəxslərin məxfiliyini poza və şəxsi təhlükəsizliyinə zərər vura bilər. Kiberhücumlar şəxsi məlumatların oğurlanması və ya yayılması, nüfuza xələl gəlməsi, maliyyə itkisi, hətta fiziki zərərlə nəticələnə bilər [10, s.103-107].

Digər sahələrə aid təsirlər. İnformasiya müharibəsinin milli təhlükəsizliyə təsiri geniş yer alır. O, dövlət sistemlərinə, hərbi əməliyyatlara və kəşfiyyat orqanlarının bütövlüyünə zərər vura bilər. Bu istiqamətdə bəzi əsas təsirlərə aşağıdakılar aid edilir:

– müdafiə sistemlərinin zəiflədilməsi. İnformasiya müharibəsi hərbi şəbəkələri hədəf alaraq, məxfi məlumatları əldə edə, komandanlıq və idarəetmə imkanlarına zərər vuraraq, müdafiə sistemlərinin fəaliyyətini sarsıda bilər. Beləliklə, bir dövlətin təhlükəsizlik təhdidlərinə effektiv cavab vermək qabiliyyətinə maneə yarada bilər.

– hibrid müharibə. İnformasiya müharibəsi çox vaxt ənənəvi hərbi taktikaları qeyri-hərbi üsullarla birləşdirilərək, hibrid müharibə strategiyalarının bir hissəsi kimi istifadə olunur. Hibrid müharibə fonunda hərbi və qeyri-hərbi sahələrin mürəkkəb qarşılıqlı fəaliyyəti milli təhlükəsizliyə öz təsirini göstərir [11].

– kritik milli infrastruktur üçün təhdidlər. İnformasiya müharibəsi elektrik şəbəkələri, nəqliyyat şəbəkələri və rabitə sistemləri də daxil olmaqla, kritik milli infrastruktur üçün əhəmiyyətli risklər yaradır. Sistemlərin fəaliyyətlərinin məhdudlaşdırılması və ya pozulması milli və ictimai təhlükəsizliyə, həmçinin iqtisadi sabitliyə ardıcıl təsir göstərir [4].

İnformasiya müharibəsi milli təhlükəsizlik fonunda siyasi, iqtisadi, sosial və digər sahələrə təsir edir, idarəetmə, demokratik proseslər, iqtisadi sabitlik, cəmiyyətin birliyi və hərbi hazırlıq üçün potensial problemlər yaradır [12]. Bu təsirləri nəzərə alaraq, milli təhlükəsizlik maraqlarını qorumaq üçün effektiv strategiyalar və əks-tədbirlər planı işlənib hazırlanmalıdır. Dövlətlərarası və beynəlxalq əməkdaşlıq, kibertəhlükəsizliyin təkmilləşdirilməsi, media savadlılığı proqramları, təkmilləşdirilmiş qanunvericilik bazaları informasiya müharibəsi təhdidləri qarşısında risklərin azaldılması, xalqların təhlükəsizliyinin təmin edilməsi və sabitliyin qorunub saxlanması üçün vacibdir.

İnformasiya müharibəsinə qarşı mübarizə strategiyaları

Rəqəmsal dünyada informasiya hökmranlığı uğrunda gedən mübarizənin milli təhlükəsizliyə təsirləri danılmazdır. İnformasiya müharibəsinin geniş vüsət alması məlumatların manipulyasiyası, yayılması və istismarına qarşı effektiv strategiyalara ehtiyac olduğunu göstərir. Bu bölmədə proaktiv tədbirləri, müdafiə mexanizmlərini və birgə səyləri əhatə edən informasiya müharibəsinə qarşı mübarizə üçün bir-biri ilə sıx əlaqəli bir sıra strategiyalar tədqiq olunur.

Maarifləndirmə və təhsil. Maarifləndirmə və təhsilin təşviqi informasiya müharibəsinə qarşı mübarizə üçün mühüm strategiyadır. Vətəndaşlar arasında media savadlılığı, tənqidi düşüncə və rəqəmsal savadlılığın artırılması nəticəsində fərdlər yalan və ya yanlış məlumatı müəyyən və ayırd etmək üçün daha məlumatlı olur. Təhsil proqramları fərdlərə mənbələri necə qiymətləndirməyi, məlumatı, faktları yoxlamağı və məzmunu tənqidi təhlil etməyi öyrənməyə imkan verir. Dövlət, təhsil müəssisələri və vətəndaş cəmiyyəti təşkilatları media savadlılığının təşviqi üçün resurs və kampaniyaların təmin edilməsində mühüm rol oynayır. Bundan əlavə, media savadlılığının və rəqəmsal vətəndaşlıq təhsilinin təşviqi informasiya müharibəsinə qarşı mübarizədə uzunmüddətli strategiya hesab edilir. Bu təhsil təşəbbüsləri tənqidi düşünmə bacarıqları, media savadlılığı və etik "onlayn" davranışı inkişaf etdirmək üçün müxtəlif yaş qruplarını hədəf alaraq, tədris müəssisələrinin kurikulumlarına inteqrasiya edilməlidir. Media savadlılığı proqramları fərdlərə etibarlı mənbələri necə müəyyən etməyi, məlumatı düzgün qiymətləndirməyi, manipulyasiya üsullarını aşkarlamağı və rəqəmsal platformalarda məsuliyyətlə naviqasiya etməyi öyrədir. Bu, fərdlərə informasiyanın məlumatlı istehlakçısı və informasiya müharibəsinə qarşı mübarizədə fəal iştirakçı olmaq imkanını verir.

Əməkdaşlıq və tərəfdaşlıq. İnformasiya müharibəsi beynəlxalq əməkdaşlıq və koordinasiya tələb edən transmilli çağırışdır. Dövlətlər və beynəlxalq təşkilatlar informasiya müharibəsi ilə kollektiv şəkildə mübarizədə normalar, qanunlar və vahid çərçivələrin yaradılması üçün kəşfiyyat məlumatlarının mübadiləsi, kiberhücumlara cavab tədbirlərinin əlaqələndirilməsi, informasiya məkanında məsuliyyətli davranışın təşviqi sahəsində əməkdaşlıq etməlidir. İnformasiya müharibəsinə qarşı mübarizədə beynəlxalq əməkdaşlığı inkişaf etdirmək üçün dialoq və əməkdaşlıq platformaları yaradılmalıdır. Bundan əlavə, informasiya müharibəsinə qarşı mübarizədə dövlətlər, kəşfiyyat agentlikləri, texnologiya

şirkətləri, vətəndaş cəmiyyəti təşkilatları arasında əməkdaşlıq və tərəfdaşlığın olması zəruridir. Bu tərəfdaşlıqlar məlumat mübadiləsi, səylərin əlaqələndirilməsi və informasiya müharibəsi təhdidlərinə birgə cavab tədbirlərini özündə cəmləşdirir. Əməkdaşlıq təşəbbüsləri kəşfiyyat xarakterli məlumatların paylanılması, birgə araşdırmaların aparılması, texnoloji həllərin işlənib hazırlanması və informasiya müharibəsini kollektiv şəkildə həll etmək üçün siyasət çərçivələrinin həyata keçirilməsini əhatə edə bilər.

Kibertəhlükəsizlik tədbirlərinin gücləndirilməsi. İnformasiya müharibəsinə qarşı mübarizədə əsas strategiyalardan biri sayılır. Qabaqcıl şifrləmə üsullarının, güclü audentifikasiya protokollarının, müdaxilənin aşkarlanması sistemlərinin və təhlükəsizlik auditlərinin tətbiqi kimi gücləndirilmiş kibertəhlükəsizlik tədbirləri informasiya sistemləri, şəbəkələri və kritik infrastrukturu kiberhücumlardan qoruyur. Müntəzəm qiymətləndirmələr və monitorinq sistemi zəif tərəfləri müəyyən etməyə və riskləri azaltmağa kömək edir. Dövlətlər, özəl sektor və beynəlxalq təşkilatlar arasında əməkdaşlıq kibertəhlükəsizlik sahəsində mükəmməl təcrübələrin işlənib hazırlanması və icrasında mühüm əhəmiyyət kəsb edir.

Əks-təbliğat və strateji ünsiyyət. Dezinformasiya, təbliğat və manipulyasiyaya qarşı proaktiv kommunikasiya strategiyalarının işlənib hazırlanması informasiya müharibəsinə qarşı mübarizədə çox vacibdir. Effektiv əks-təbliğat yalan məlumatların aşkarlanması, doğru məlumatın təbliği və manipulyasiya üsullarını ifşa etməyi özündə birləşdirir. Dövlətlər və təşkilatlar şəffaf və etibarlı kommunikasiya kanalları vasitəsilə ənənəvi və rəqəmsal media platformalarından istifadə edərək, düzgün məlumat vermək və problemləri operativ şəkildə həll etmək üçün ictimaiyyətlə əlaqə saxlamalıdır. İnformasiya müharibəsinin təsirlərinə qarşı mübarizədə ictimai etimadın və qarşılıqlı əlaqənin yaradılması vacibdir.

Tədqiqat və inkişaf. Tədqiqat və inkişafa sərmayə qoymaq informasiya müharibəsinə qarşı mübarizədə olduqca vacibdir. Dövlətlər, özəl sektor qurumları və akademik dairələrdə yaranan təhlükələri araşdırmaq, qabaqcıl texnologiyaları inkişaf etdirmək, informasiya müharibəsi taktikalarını müəyyənləşdirmək və onlara adekvat cavab vermək üçün analitik imkanları artırmaq məqsədilə resurslar ayırmalıdır. Tədqiqat zamanı informasiya müharibəsinin təsirini aşkar və təhlil edə, həmçinin effektivliyini aşağı sala bilən vasitə və texnikalar hazırlamaq üçün süni intellekt, məlumat analitikası və maşının öyrənilməsi kimi sahələrə diqqət yetirilməlidir.

Qanunvericilik və siyasət çərçivələri. İnformasiya müharibəsinə qarşı mübarizə üçün dayanıqlı qanunvericilik və siyasət çərçivələrinin hazırlanması zəruridir. Qanunlar dezinformasiyanın yayılması, şəxsi həyatın toxunulmazlığının qorunması, kibercinayətkarlıq və seçkilərə müdaxilə kimi məsələlərin hüquqi bazasının olması vacibdir. Dövlətlər, həmçinin məzmunun moderasiyası, alqoritmlərdə şəffaflıq və məlumat mübadiləsi üçün təlimatlar və standartların yaradılmasında texnologiya şirkətləri ilə birgə fəaliyyət göstərilməlidir.

Beynəlxalq norma və standartlar. İnformasiya müharibəsinə qarşı mübarizədə informasiya məkanında məsuliyyətli davranış qaydaları, kritik infrastrukturu hədəf alan kiberhücumlara qarşı normalar və məlumat mübadiləsi, əməkdaşlıq haqqında sazişlərin yaradılması kimi beynəlxalq norma və standartları təşviq etmək üçün səylər göstərilməlidir. Birləşmiş Millətlər Təşkilatı (BMT) və regional qurumlar kimi beynəlxalq təşkilatlar dialoqun təşviqində, normaların işlənib hazırlanmasında və millətlərarası əməkdaşlığın asanlaşdırılmasında mühüm rol oynayır.

Davamlı monitorinq və qiymətləndirmə. Hazırlanan strategiyaları uyğunlaşdırmaq və təkmilləşdirmək üçün əks-tədbirlərin effektivliyinin monitorinqi və qiymətləndirilməsi vacibdir. Dövlətlər və təşkilatlar informasiya müharibəsi fəaliyyətlərinə nəzarət etmək, əks-tədbirlərin təsirini qiymətləndirmək və yaranan təhlükələri müəyyən etmək üçün mexanizmlər hazırlamalıdır. Müntəzəm qiymətləndirmələr strategiyaların daim inkişaf edən informasiya məkanında aktual və effektiv qalmasını təmin edir.

İnformasiya müharibəsinə qarşı mübarizə fəal tədbirləri, müdafiə mexanizmlərini və birgə səyləri birləşdirən çoxşaxəli yanaşmanı tələb edir. Yuxarıda göstərilən yanaşmalar effektiv əks-informasiya müharibəsi strategiyasının mühüm komponentləridir. Bu strategiyaları həyata keçirməklə dövlətlər,

təşkilatlar və fərdlər informasiya müharibəsinin yaratdığı riskləri azaltmaq, milli təhlükəsizlik təhdidini aradan qaldırmaq və informasiya ekosistemlərinin bütövlüyünü saxlamaq məqsədilə birgə fəaliyyət göstərə bilərlər.

Tədqiqat istiqaməti: real dünya nümunələri

İnformasiya müharibəsinin real dünya nümunələri bu fenomenin mürəkkəbliyi və milli təhlükəsizliyə təsirləri haqqında hərtərəfli fikirlərin formalaşması üçün əhəmiyyətlidir. Bu nümunələrin araşdırılması tətbiq olunan taktikaları, onların müxtəlif sahələrə təsirini və informasiya müharibəsinə qarşı mübarizədə çətinlikləri dərk etməyə kömək edir. Bu bölmədə informasiya müharibəsi ilə milli təhlükəsizliyin kəsişməsini göstərən vacib nümunələr tədqiq olunur.

1. Rusiyanın 2016-cı il ABŞ prezident seçkilərinə müdaxiləsi. Bu hal informasiya müharibəsi haqqında mühüm fikirlərin yaranmasına gətirib çıxarır. Sosial media manipulyasiyası, hakerlik və dezinformasiya kampaniyaları vasitəsilə rus aktorlar ictimai rəyə təsir etmək, nifaq salmaq və demokratik proseslərə olan inamı sarsıtmaq məqsədi güdürdülər. Yalan xəbərlərin yayılması, məqsədyönlü mesajlaşma və siyasi disbalansın gücləndirilməsi informasiya müharibəsinin seçki sistemlərinə və demokratik institutlara potensial təsiri qaçılmaz etdi [13].

2. Kritik infrastruktura kiberhücumlar. 2010-cu ildə kəşf edilən “Stuxnet” adlı kompüter qurdu kritik infrastrukturu hədəfə alan informasiya müharibəsi ilə bağlı əhəmiyyətli nümunədir. Birləşmiş Ştatlar və İsrailin birgə hazırladığı “Stuxnet” xüsusilə İranın nüvə obyektlərini hədəfə almışdı. Kompüter qurdu sənaye nəzarət sistemlərini sıradan çıxardaraq, sentrifuqlara ziyan vurmuş və İranın nüvə zənginləşdirmə imkanlarına ciddi maneə yaratmışdır. Bu nümunə araşdırıldığı zaman onun informasiya müharibəsinin kritik infrastruktura potensial təsiri və hücumların anonimliyi kimi çətinliklər ortaya çıxır [14].

3. İŞİD-in təbliğatı və terrorçuluğa cəlb edilməsi. İŞİD təbliğat kampaniyaları və sosial media platformaları vasitəsilə ekstremist ideologiyaları yaymaq, zorakılıq hərəkətlərini nümayiş etdirmək və dünyanın müxtəlif yerlərindən insanları öz sıralarına cəlb etmək məqsədinə nail olmağa çalışır. Bu nümunənin araşdırılmasında məqsəd fərdləri radikallaşdırmaqda, zorakılığı qızışdırmaqda və əhəmiyyətli milli təhlükəsizliyə təhdid yaratmaqda olan informasiya müharibəsinin gücünü göstərməkdən ibarətdir [15].

4. Seçkilərdə dezinformasiya kampaniyaları. Müxtəlif ölkələrdə, o cümlədən Fransa və Almaniyada müşahidə olunan bu kampaniyalar yalan məlumatların yayılmasını, məlumatların manipulyasiyasını və seçki nəticələrinə təsir etmək üçün süni “onlayn” personajların yaradılmasını nəzərdə tutur. Burada məqsəd, şübhə və fikir ayrılığı yaratmaq, demokratik proseslərə ictimai inamı sarsıtmaqdır. Bu nümunə araşdırmaları seçki sistemlərinin və demokratik təsisatların bütövlüyünü qorumaq üçün informasiya müharibəsinə qarşı mübarizənin vacibliyini vurğulayır [16].

5. Çinin kibercasusluq əməliyyatları. Çinin kibercasusluq fəaliyyəti milli təhlükəsizlik baxımından digər dövlətlərə ciddi problemlər yaradır. Çin aktorlar bütün dünyada dövlət qurumlarını, müdafiə sənayesi şirkətlərini və tədqiqat institutlarını hədəfə alan müxtəlif haker qruplarından ibarətdir. Bu kiberəməliyyatlar həssas məlumatları, əqli mülkiyyəti oğurlamaq və strateji üstünlüklər əldə etmək məqsədi daşıyır. 2015-ci ildə ABŞ-ın milyonlarla federal əməkdaşının şəxsi məlumatlarının ələ keçirildiyi “Personal İdarəetmə Ofisi” fəaliyyətinin məhdudlaşdırılması fonunda baş vermiş hadisə informasiya müharibəsinin milli təhlükəsizliyə təsirini və güclü kibertəhlükəsizlik tədbirlərinə zərurət olduğunu göstərir [2].

6. Ukraynada hibrid müharibə. Ukraynadakı münaqişəni informasiya müharibəsi elementlərini özündə birləşdirən hibrid müharibə nümunəsi kimi görmək olar. Rusiya Ukraynanın şərqindəki separatçı hərəkatları dəstəkləmək üçün hərbi güc, təbliğat, dezinformasiya kampaniyaları və kiberhücumlardan istifadə edirdi. Yalan məlumatların yayılması, manipulyasiyası və Ukrayna infrastrukturunu hədəf alan kiberhücumlar informasiya müharibəsi taktikalarının ənənəvi hərbi strategiyalara inteqrasiyasını nümayiş etdirir [17].

Real dünya nümunələri informasiya müharibəsinin milli təhlükəsizliyə təsiri haqqında dəyərli fikirləri özündə ehtiva edir. Yuxarıda qeyd olunan nümunələr informasiya müharibəsinin müxtəlif taktika və nəticələrini əks etdirir. Bu araşdırmalar informasiya müharibəsinə qarşı mübarizədə çətinlikləri, məsələn, yalan məlumatın sürətlə yayılması və ictimai rəyin manipulyasiyasını tədqiq edir. Dövlətlər və tərəflərarası əməkdaşlıq, gücləndirilmiş kibertəhlükəsizlik tədbirləri, media savadlılığı proqramları, beynəlxalq əməkdaşlıq və möhkəm qanunvericilik bazalarının inkişafı daxil olmaqla, effektiv strategiyalar informasiya müharibəsinin yaratdığı təhlükələrə qarşı mübarizədə mühüm əhəmiyyət kəsb edir. Bu istiqamətdə dünyada baş vermiş insidentləri öyrənməklə, dövlətlər informasiya müharibəsinin mürəkkəbliklərini daha yaxşı anlaya və milli təhlükəsizlik maraqlarının qorunması üçün hərtərəfli yanaşmalar inkişaf etdirə bilər.

Nəticə

İnformasiya müharibəsinin milli təhlükəsizliyə əsas təhdid kimi ortaya çıxması onun konseptual əsasları, təsirləri, ona qarşı mübarizə strategiyaları və real dünya nümunələrinin hərtərəfli başa düşülməsini tələb edir. Bu məqalə Milli təhlükəsizlik maraqlarının qorunmasında informasiya müharibəsi ilə mübarizənin əhəmiyyəti məqalədə vurğulanmış və müvafiq aspektləri işıqlandırmışdır.

İnformasiyanın manipulyasiyası və istismarı ilə səciyyələnən informasiya müharibəsi siyasi, iqtisadi və sosial sahələrə geniş təsir göstərir. O, demokratik prosesləri sarsıdır, kritik infrastrukturun fəaliyyətinə zərər vurur və ictimai inamı sarsıdır. Texnologiyanın sürətli təkamülü və rəqəmsal dünyanın qarşılıqlı əlaqəsi informasiya müharibəsinə qarşı mübarizə ilə əlaqəli problemləri daha da gücləndirir. Bu təhlükəni effektiv həll etmək üçün informasiya müharibəsinə qarşı mübarizə strategiyaları fəal, əməkdaşlıq çərçivəsində qurulmalı və çoxölçülü olmalıdır. Kritik infrastrukturu və informasiya sistemlərini kiberhücumlardan qorumaq üçün kibertəhlükəsizlik tədbirlərinin gücləndirilməsi vacib amillərdən hesab olunur. Media savadlılığının və rəqəmsal vətəndaşlıq təhsilinin təşviqi fərdlərə məlumatları tənqidi qiymətləndirməyə və manipulyasiya üsullarını aşkar etməyə imkanı verir. Beynəlxalq əməkdaşlıq məlumat mübadiləsini, birgə cavabları, norma və çərçivələrin yaradılmasını asanlaşdırır. Əks-təbliğat və strateji kommunikasiya təşəbbüsləri yalan məlumatların üzə çıxarılmasında və düzgün məlumatın təbliğində mühüm rol oynayır.

Real dünya nümunələri informasiya müharibəsinin milli təhlükəsizliyə təsirinin konkret nümunələrini özündə əks etdirir. Bu nümunə araşdırmaları informasiya müharibəsinə qarşı effektiv mübarizə aparmaq üçün adaptiv və hərtərəfli strategiyalara olan zərurəti tədqiq edir.

Nəticə olaraq, informasiya müharibəsinə qarşı mübarizə fəal tədbirlər, birgə səylər və davamlı adaptasiya tələb edən mürəkkəb və çoxşaxəli prosesdir. Dövlətlər, təşkilatlar və fərdlər kibertəhlükəsizlik tədbirlərini gücləndirməli, media savadlılığını və beynəlxalq əməkdaşlığı təşviq etməli, effektiv əks-tədbirlər görməlidir. Bu fəaliyyətlərin həyata keçirilməsi milli təhlükəsizlik maraqlarını və informasiya ekosistemlərinin bütövlüyünü qoruya, qloballaşan dünyada xalqların sabitliyi və rifahını təmin edə bilər.

İstifadə edilmiş ədəbiyyat siyahısı

1. Brazzoli, M.S. Future prospects of information warfare and particularly psychological operations // – South African army vision, – 2020, – p. 217-232.

2. Grages, T.H. Playing the Long Game: How Cyber Will Facilitate China's Long-Term Economic Espionage Campaign and Information Warfare Objectives: / PhD diss. / – Utica College, 2020 – 130 p.

3. Bolton, D. Targeting ontological security: Information warfare in the modern age // Political psychology, – 2021. № 1 (42) – p. 127-142.

4. Taddeo, M. Information warfare: A philosophical perspective // Philosophy and Geography, – 2011. №1 (25) – p. 105-120.

5. Paterson, T., Lauren, H. Political warfare in the digital age: cyber subversion, information operations and ‘deep fakAustralian Journal of International Affairs, – 2020. №4 (74). – p. 439-454.

6. Bârgăoanu, A. Godzimirski, J., Ioniță D. Information Warfare and information operations in the black sea area // – New Strategy Center, Norwegian Institute of International Affairs, – 2020, p. 3-34.
7. Usmonov, M. Information War // – International Journal of Academic and Applied Research (IJAAR), –2021. №1 (5). – p. 79-82.
8. Harknett, R.J and Max S. Cyber campaigns and strategic outcomes // – Journal of Strategic Studies, – 2022. №4 (45) – p. 534-567.
9. Acton, J.M. Cyber warfare & inadvertent escalation // – Daedalus, – 2020. №2 (149). – p. 133-149.
10. Christopher, W. In Information warfare in the age of cyber conflict. Social media as information warfare / W.Christopher, T.Trevor, M.M.Brian, J.Prier – Abingdon, Oxfordshire: Published by Routledge, – 2020. – 270 p.
11. Clark, M. Russian hybrid warfare // – Washington, DC: Institute for the Study of War – 2020, – p. 8-33.
12. A.H.Həsənov, R.R.İmanov, V.Z.İsayeva. Hibrid müharibələrdə informasiya hücumları // Strateji təhlil jurnalı, Bakı, 2018, № 1-2 (23-24), s. 485-495.
13. McCombie.S, Allon.J.U, Morrison, S. The US 2016 presidential election & Russia's troll farms // – Intelligence and National Security, – 2020, №1 (35). – p. 95-114.
14. Plėta,T., Tvaronavičienė, M., Silvia, D.C., Agafonov, K. Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases // – Vilnius: Entrepreneurship and Sustainability Center, – 2020.№3(2) – p. 703-715.
15. Mitts, T., Gregoire, P., Barbara, F.W. Studying the impact of ISIS propaganda campaigns // – The Journal of Politics, – 2022. №2 (84). – p. 1220-1225.
16. Baumann, M. Propaganda Fights' and 'Disinformation Campaigns': the discourse on information warfare in Russia-West relations – Contemporary Politics, – 2020. №3 (26) – p. 288-307.
17. Bachmann, S.D, Dries, P., Duczynski, G. Hybrid warfare and disinformation: A Ukraine war perspective // – Global Policy, – 2023. №2 (14). – p. 3-5.

Аннотация
Информационная война и национальная безопасность
Рашадат Оруджев

В статье на реальных примерах отражены роль информационной войны в национальной безопасности, концептуальный взгляд на информационную войну, влияние информационной войны на национальную безопасность, стратегии борьбы с информационной войной. Рассматривается важность использования информационных и коммуникационных технологий для получения преимущества в конфликтах или достижения стратегических целей, а также манипулирования, эксплуатации и распространения информации с целью отрицательного воздействия на функционирование стратегических коммуникационных систем и влияния на результаты, а также борьба за информационное превосходство в контексте национальной безопасности. Объясняется, что оно играет решающую роль. Основная цель данного исследования – повышение медиаграмотности, критического мышления и цифровой грамотности граждан, а также формирование у личности способности выявлять и отличать ложную информацию. В этих рамках образовательные программы позволяют людям научиться оценивать источники, проверять информацию, факты и критически анализировать контент. В статье также упоминается сотрудничество государств и международных организаций в области обмена информацией, координации реагирования на кибератаки и продвижения ответственного поведения в информационном пространстве для создания норм, законов и единых рамок коллективной борьбы с информационной войной.

Ключевые слова: стратегическая коммуникация, национальная безопасность, информационная война, коммуникационные технологии, обмен информацией

Abstract
Information warfare and national security
Rashadat Orujov

In the article, the role of information warfare in national security, a conceptual view of information warfare, the impact of information warfare on national security, and strategies for combating information warfare are reflected in real-world examples. The importance of using information and communication technologies to gain advantage in conflicts or achieve strategic goals, as well as the manipulation, exploitation, and dissemination of information to adversely affect the functioning of strategic communication systems and influence outcomes, are addressed, and the struggle for information superiority in the context of national security. It is explained that it plays a decisive role. The main goal of this study is to increase media literacy, critical thinking and digital literacy among citizens, and to form the ability to identify and distinguish false information in individuals. In this framework, educational programs enable individuals to learn how to evaluate sources, check information, facts, and critically analyze content. The article also mentions the cooperation of states and international organizations in the field of information sharing, coordination of responses to cyber attacks, and promotion of responsible behavior in the information space for the creation of norms, laws and unified frameworks for the collective fight against information warfare.

Keywords: strategic communication, national security, information warfare, communication technologies, information exchange

Məqalə redaksiyaya daxil olmuşdur:25.04.2024
Təkrar işlənməyə göndərilmişdir:06.05.2024
Çapa qəbul edilmişdir: 03.06.2024