Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№1(11)/2025, səh. 97-112

MİLLİ TƏHLÜKƏSİZLİK ***NATIONAL SECURITY***

UOT 355.4, 004.056, 327.8 DOI: 10.30546/mk.2024.4.0125

HİBRİD TƏHDİDLƏR VƏ AZƏRBAYCANIN MÜDAFİƏ STRATEGİYASI

polkovnik-leytenant Vüqar Şirinov
Daxili İşlər Nazirliyi Daxili Qoşunlarının Hərbi İnstitutu
vugarshirinov.office@gmail.com.

Xülasə. Bu məqalədə ölkələrin təhlükəsizlik mühitində önəmli yer tutan hibrid təhdidlərin mahiyyəti, onların milli təhlükəsizlik üçün yaratdığı təhlükələr və bu təhdidlərə qarşı tətbiq olunan müdafiə strategiyaları təhlil edilir.

Hibrid təhdidlər ənənəvi hərbi taktikalarla yanaşı, kiberhücumlar, dezinformasiya kampaniyaları, iqtisadi təzyiq vasitələri, eləcə də süni intellekt və sosial mühəndislik kimi yeni nəsil manipulyasiya texnologiyalarından istifadə edərək dövlətlərə qarşı təsir vasitəsi kimi tətbiq edilir. Geosiyasi mövqeyi, enerji resursları və regional münaqişələr səbəbindən Azərbaycan hibrid təhdidlərə məruzqalma riski yüksək olan ölkələrdəndir. Bu kontekstdə hibrid təhdidlərə qarşı kompleks müdafiə strategiyası çərçivəsində milli təhlükəsizlik siyasəti, kibertəhlükəsizlik tədbirləri, dezinformasiyaya qarşı mübarizə və beynəlxalq əməkdaşlıq imkanları ətraflı təhlil edilir.

Məqalədə, həmçinin hibrid təhdidlərə qarşı qabaqcıl ölkələrin tətbiq etdiyi müdafiə modelləri araşdırılmış və bu təcrübələrin Azərbaycan üçün tətbiq oluna biləcək aspektləri müəyyən edilmişdir.

Açar sözlər: hibrid təhdidlər, müdafiə strategiyası, milli təhlükəsizlik, kibertəhlükəsizlik, beynəlxalq əməkdaşlıq, asimmetrik müharibə

Giriş

Müasir təhlükəsizlik mühitində ənənəvi hərbi müdaxilələrlə yanaşı, qeyri-ənənəvi metodlarla həyata keçirilən və dövlətlərin sabitliyini, suverenliyini təhdid edən yeni təhlükə növləri geniş yayılmağa başlamışdır. Bu kontekstdə, "hibrid təhdid" termini ilk dəfə 2007-ci ildə Amerika Birləşmiş Ştatlarının dəniz piyadası qüvvələrinin generalı Ceyms Mettis və hərbi analitik Frank Hoffman tərəfindən istifadə edilmişdir [1]. Hibrid təhdidlər kiberhücumlar, dezinformasiya kampaniyaları, iqtisadi təzyiq və digər qeyri-hərbi vasitələrlə milli maraqlara təsir göstərməklə dövlətlərin təhlükəsizlik sistemlərini sarsıtmaq və onları zəiflədib təsir altına almaq məqsədilə ənənəvi və qeyri-ənənəvi mübarizə üsullarının birgə tətbiqinə əsaslanan kompleks təhlükələrdir.

Azərbaycanın strateji coğrafi mövqeyi, malik olduğu enerji resursları, meqalayihələrdə iştirakı, Cənubi Qafqazda nüfuzlu dövlət kimi rolu regiondakı əhəmiyyətini artırır, həmçinin onu müəyyən xarici qüvvələr üçün maraqlı və eyni zamanda geosiyasi təzyiqlərə açıq bir hədəfə çevirir. Ermənistan ilə uzun müddət davam edən münaqişə və Azərbaycanın suverenliyinə qarşı olan digər təhdidlər ölkənin təhlükəsizlik mühitini daha da mürəkkəbləşdirir. Ermənistanın və bəzi xarici aktorların dəstəklədiyi dezinformasiya kampaniyaları, kiberhücumlar və daxili qeyri-sabitlik yaratmaq cəhdləri Azərbaycan əleyhinə hibrid təhdidlərin elementləri kimi qəbul edilə bilər. Xarici qüvvələr bu təhdidlərdən istifadə edərək Azərbaycanın siyasi və iqtisadi qərarlarına öz maraqlarına uyğun şəkildə təsir göstərməyə çalışırlar.

Bu cür mürəkkəb təhlükəsizlik mühitində Azərbaycanda hibrid təhdidlərə qarşı mübarizənin gücləndirilməsinə, dövlətin regional və beynəlxalq səviyyədə mövqeyinin möhkəmləndirilməsinə, həmçinin səmərəli müdafiə sistemlərinin qurulmasına istiqamətlənmiş kibertəhlükəsizlik tədbirlərini, beynəlxalq əməkdaşlığı və diplomatik əlaqələri əhatə edən kompleks müdafiə strategiyası hazırlanmışdır. Hibrid təhdidlərin qarşısını almaq və milli təhlükəsizliyi təmin etmək, eləcə də təhlükəsizlik tədbirlərini daha səmərəli şəkildə təşkil etmək məqsədilə Azərbaycan Respublikasının Milli Məclisi 30 sentyabr 2024-cü ildə xarici müdaxilələrə və hibrid təhdidlərə qarşı mübarizə üzrə

xüsusi komissiya yaratmışdır [2]. Komissiyanın yaradılması Azərbaycanın hibrid təhdidlərə qarşı müdafiə strategiyasının gücləndirilməsi məqsədilə atılan əhəmiyyətli addımlardan biridir.

Məqalənin yazılmasında məqsəd hibrid təhdidlərin mahiyyətini və onların milli təhlükəsizliyə yaratdığı təhlükələri, o cümlədən Azərbaycanın hibrid təhdidlərə qarşı həyata keçirdiyi mübarizə tədbirlərini və bu sahədə tətbiq olunan yanaşmaların effektivliyini təhlil etmək, həmçinin hibrid təhdidlərin doğurduğu təhlükələri nəzərə alaraq, mövcud strategiyaların davamlılığı və gələcək inkişaf perspektivləri araşdırmaqdır.

Araşdırmada analitik metoddan istifadə edilmişdir ki, bu da hibrid təhdidlərin fərqli aspektlərini ayrılıqda incələməyə və onların milli təhlükəsizliyə təsirini dərindən təhlil etməyə imkan verir.

Hibrid təhdidlərin əsas elementləri

Hibrid təhdidlər dövlətlər və ya qeyri-dövlət aktorları tərəfindən siyasi, iqtisadi, hərbi və informasiya sahələrində maraqlarını təmin etmək məqsədilə ənənəvi və qeyri-ənənəvi metodların kompleks şəkildə tətbiq edilməsidir. Bu cür strategiyalar hədəf dövlətlərin zəif nöqtələrindən istifadə edərək daxili sabitliyi pozmağa, eyni zamanda beynəlxalq nüfuzunu zəiflətməyə yönəlmişdir. Hibrid təhdidlər çoxşaxəli vasitə və metodların kombinasiyası ilə həyata keçirilir. Onların əsas tətbiq mexanizmləri arasında aşağıdakı üsullar xüsusi yer tutur:

Kiberhücumlar. Hibrid təhdidlərin ən mühüm elementlərindən biri kiberməkan üzərində icra olunan hücum və manipulyasiyalardır. Kiberməkan informasiya və kommunikasiya texnologiyalarının qarşılıqlı əlaqəsi nəticəsində yaranan rəqəmsal və virtual bir mühitdir. O, şəbəkələr, kompüter sistemləri, bulud texnologiyaları və digər rəqəmsal platformaları əhatə edərək məlumat mübadiləsi və kommunikasiya proseslərini təmin edir. Bu mühit fiziki sərhədlərdən azaddır və real dünya ilə sıx qarşılıqlı əlaqədədir. Müasir dövrdə kiberməkan təkcə texnoloji yeniliklərin tətbiq sahəsi kimi deyil, həm də iqtisadiyyatın, dövlət idarəetmə proseslərinin, ticarət əməliyyatlarının və fərdi azadlıqların təmin olunmasında mühüm əhəmiyyət daşıyan strateji bir sahədir. Dövlətlər və təşkilatlar kiberməkanı idarəetmə, strateji resursların qorunması və təhlükəsizliyin təmin olunması üçün əsas platforma kimi istifadə edirlər. Kiberməkanın təhlükəsizliyi yalnız fərdi məlumatların qorunması deyil, həm də dövlətlərin milli təhlükəsizliyinin təmin olunması baxımından vacibdir. Bu səbəbdən kiberməkanın müdafiəsi müasir dövrdə həm dövlətlərin, həm də beynəlxalq təşkilatların prioritetlərindən biri hesab olunur [3].

Kiberməkanın strateji əhəmiyyəti, onu hibrid təhdidlərin mühüm elementlərindən biri olan kiberhücumların hədəfinə çevirir. Kiberhücumlar yalnız texnoloji ziyanla məhdudlaşmır. Onlar iqtisadi sistemlərə, ictimai sabitliyə və dövlətlərin strateji qərar qəbuletmə mexanizmlərinə də ciddi təsir göstərir. Kiberməkandan asılı olan müasir cəmiyyətlər üçün belə hücumlar iqtisadi və siyasi sabitliyi təhlükə altına alır. Kiberməkanın riskləri fonunda kiberhücumlara qarşı effektiv mübarizə üçün informasiya təhlükəsizliyinin təmin olunması, qabaqlayıcı texnologiyaların tətbiqi və ictimaiyyətin məlumatlandırılması həyati əhəmiyyət daşıyır.

Dezinformasiya və informasiya müharibəsi. Dezinformasiya və informasiya müharibəsi müasir dövrdə hibrid təhdidlərin ən mürəkkəb formalarından biri olaraq dövlətlərin siyasi, iqtisadi və sosial sabitliyinə ciddi təhlükə yaradır. Dövlətlər və qeyri-dövlət aktorları bu vasitələrdən ictimai rəyi manipulyasiya etmək, dezinformasiya yaymaq və strateji qərar qəbuletmə prosesinə təsir göstərmək məqsədilə istifadə edirlər [4]. İnformasiya müharibəsinin əsas alətləri arasında saxta məlumatların sosial media və kütləvi informasiya vasitələrində geniş yayılması, manipulyativ məzmunların yaradılması, hədəf auditoriyaların psixoloji təsirə məruz qalması üçün xüsusi mesajların hazırlanması və onların təsirinin artırılması məqsədilə rəqəmsal texnologiyalardan istifadə yer alır. Belə kampaniyalar müəyyən məqsədləri həyata keçirmək üçün effektiv vasitə hesab olunur və aşağıdakı istiqamətlərdə özünü göstərir:

1. İctimai sabitliyin pozulması: xarici aktorlar tərəfindən idarə olunan dezinformasiya kampaniyaları ictimai rəyi manipulyasiya etməklə cəmiyyətin müxtəlif təbəqələri arasında parçalanma yaradır və sosial narazılığı dərinləşdirir.

2. Strateji təsir: dezinformasiyadan istifadə edərək dövlətlərin xarici siyasətində və beynəlxalq münasibətlərində qərar qəbuletmə mexanizmlərinə müdaxilə olunur. Belə yanaşmalar, xüsusilə geosiyasi münaqişələr zamanı daha da güclənir.

3. Beynəlxalq imicin zəiflədilməsi: informasiya müharibəsi dövlətlərin beynəlxalq aləmdəki reputasiyasını sarsıtmağa yönəldilir. Bu da beynəlxalq təşkilatlar və tərəfdaşlarla münasibətlərin pozulmasına və xarici investisiyaların azalmasına səbəb olur.

Sosial media platformaları informasiya müharibəsində məlumatın sürətlə yayılması, saxta hesablar vasitəsilə kütləvi manipulyasiya aparılması və hədəf auditoriyanın təsir altına alınması üçün ən effektiv vasitələrdən biri hesab edilir. Sosial şəbəkələrdə yayılan dezinformasiya həm daxili ictimai rəydə, həm də beynəlxalq səviyyədə manipulyativ təsir yaradır [5].

İqtisadi təzyiq. İqtisadi təzyiq hibrid təhdidlərin əsas komponentlərindən biri olmaqla, dövlətlər və qeyri-dövlət aktorlarının hədəf ölkələrin daxili sabitliyini və xarici siyasətini manipulyasiya etmək üçün istifadə etdiyi effektiv vasitələrdən biridir. Bu üsul iqtisadi resurslara çıxışın məhdudlaşdırılması, strateji sektorların hədəfə alınması və ticarət əlaqələrinə maneələr yaradılması kimi geniş bir spektri əhatə edir. Bu proses strateji sahələrdə üstünlük əldə etmək məqsədilə məqsədyönlü şəkildə həyata keçirilir və əsasən aşağıdakı mexanizmlər vasitəsilə icra olunur:

– *ticarət embarqoları və sanksiyalar:* hədəf ölkənin xarici ticarətini zəiflətmək, ixrac imkanlarını məhdudlaşdırmaq və iqtisadi inkişafa mane olmaq məqsədilə istifadə edilir;

– *qiymət manipulyasiyaları:* strateji əhəmiyyətli malların, xüsusilə enerji resurslarının qiymətinin manipulyasiya edilməsi ilə hədəf ölkələrə iqtisadi təzyiq göstərilir;

– *investisiya axınının azaldılması:* xarici sərmayələrin qarşısını almaq və iqtisadi sabitliyi pozmaq üçün spesifik tədbirlər həyata keçirilir;

– *iqtisadi asılılığın artırılması:* kreditlər, maliyyə yardımları və ya ticarət sazişləri vasitəsilə hədəf ölkələrin iqtisadi siyasətinə təsir göstərilir [6].

İqtisadi təzyiq hibrid təhdidlərin əsas alətlərindən biri kimi, dövlətlərarası münasibətlərdə güc balansını dəyişdirmək üçün mühüm potensiala malikdir. Bundan istifadə edərək hədəf ölkələrə həm iqtisadi, həm də siyasi təzyiq göstərilir, onların beynəlxalq arenadakı mövqeləri zəiflədilir. İqtisadi təzyiq, eyni zamanda qlobal iqtisadi sabitlik üçün də ciddi təhdidlər yaradır. Bu cür təzyiq vasitələri iqtisadi mühitdə rəqabəti məhdudlaşdırmaqla güc balansını dəyişdirməyə və geosiyasi üstünlük əldə etməyə xidmət edir.

Vasitəçi – "proxy" qüvvələr. Hibrid təhdidlər kontekstində vasitəçi *(proxy)* qüvvələr mühüm rol oynayır. Dövlətlər birbaşa münaqişəyə daxil olmadan vasitəçi aktorlarla rəqib tərəfə təzyiq göstərir, beləliklə, beynəlxalq hüquqi məsuliyyətdən yayınır və münaqişənin miqyasını genişləndirmədən öz maraqlarını qoruyur. Bu yanaşma həmin dövlətlərin qeyri-dövlət aktorları vasitəsilə rəqib ölkələrin sabitliyini pozmaq, əhali arasında qorxu yaratmaq və regional balansı öz lehinə dəyişmək məqsədi daşıyır. Terror təşkilatları və radikal qruplar vasitəsilə həyata keçirilən belə təhdidlər rəqib dövlətlərin təhlükəsizlik sistemini sarsıtmaqla onların müdafiə və idarəetmə mexanizmlərini zəiflədir, ictimai sabitliyə ciddi zərbə vurur [7]. Bu hibrid təhdid növü birbaşa münaqişəyə qoşulmayan bir (və ya bir neçə) dövlətin münaqişə iştirakçısı olan bir aktoru dəstəkləyərək, onun vasitəsilə öz strateji maraqlarını həyata keçirməsi və potensial üstünlüklər əldə etməsi ilə xarakterizə olunur.

Vasitəçi müharibəsinin iki əsas aktoru mövcuddur:

– *əsl aktor* – adətən, böyük bir (və ya bir neçə) dövlətdir. O, birbaşa münaqişəyə qoşulmadan, vəkil aktora (dövlət, yaxud qeyri-dövlət) silah, hərbi texnika, ərzaq, eləcə də hərbi təlim və kəşfiyyat məlumatları kimi resurslar təqdim edir.

– *vəkil aktor* – əsl aktordan aldığı dəstəklə birbaşa mübarizə aparan tərəfdir. O, bir dövlət, eləcə də terror təşkilatı və ya dövlət tərəfindən dəstəklənən separatçı qruplar formasında ola bilər [8].

Vasitəçi qüvvələr həm hərbi, həm də qeyri-hərbi vasitələrlə rəqib tərəfə təzyiq göstərərək onu zəiflətməyə çalışırlar. Vasitəçi müharibələrinin bu xüsusiyyətləri onları müasir münaqişələrdə strateji alətə çevirir.

Hüquqi təzyiq – "Lawfare" təhdidləri. Beynəlxalq müstəvidə "Lawfare" termini, hüquqi vasitələrdən məqsədyönlü şəkildə istifadə edərək dövlətlərin daxili və xarici siyasətinə təsir göstərmək, beynəlxalq arenada onların "mövqeyini zəiflətmək" mənasını ifadə edir. Bu metod hibrid təhdidlərin mühüm elementlərindən biri kimi, xüsusilə siyasi, iqtisadi və hüquqi təzyiq alətləri vasitəsilə həyata keçirilir. Beynəlxalq hüquq çərçivəsində insan haqları pozuntuları və ərazi mübahisələri ilə bağlı irəli sürülən iddialar hüquqi alətə çevrilərək hədəf ölkəyə qarşı siyasi təzyiq mexanizmi kimi istifadə edilir. Ermənistanın 44 günlük müharibədən sonra Azərbaycanın hərbi əməliyyatlarını etnik təmizləmə kimi təqdim etməyə çalışması və beynəlxalq məhkəmələrə müraciət etməsi bu strategiyanın nümunəsidir. Hüquqi mexanizmlər yalnız məhkəmə iddiaları ilə məhdudlaşmır, eyni zamanda beynəlxalq təşkilatlar, müqavilələr və qətnamələr vasitəsilə də dövlətlərə siyasi təzyiq göstərmək üçün istifadə edilir. Bu yanaşma media və diplomatik kanallar vasitəsilə dezinformasiyanın legitimləşdirilməsi, dövlətlərin daxili qanunvericiliyinə müdaxilə edilməsi və guya beynəlxalq standartlara uyğunlaşdırmaq məqsədi ilə dəyişikliklərə məcbur edilməsi üçün istifadə olunur. Hüquqi təzyiq hibrid müharibənin əsas vasitələrindən biri kimi hüquq sistemlərinin siyasi alətə çevrilməsini təmin edir və dövlətlərarası rəqabətdə mühüm rol oynayır.

Yeni nəsil hibrid müharibə alətləri. Müasir dövrdə informasiya müharibəsinin tərkib hissəsi olan və dövlətlərin təhlükəsizliyinə təhdid yaradan *süni intellekt, böyük verilənlər (Big Data) analitikası, deepfake* (süni intellektlə yaradılmış saxta görüntü və ya video) texnologiyası *və sosial mühəndislik* hibrid təhdidlərin mühüm komponentləri kimi çıxış edir. Bu texnologiyalar informasiya müharibəsində effektiv vasitələrə çevrilərək, real və virtual dünyalar arasında əlaqələri daha mürəkkəb hala gətirir. Onların tətbiqi informasiya təhlükəsizliyi sahəsində yeni imkanlar yaratmaqla yanaşı, manipulyativ texnologiyaların yayılmasını sürətləndirir, kütləvi təsiri gücləndirir və dövlətlərin strateji maraqlarına yönəlmiş riskləri artırır. Bu kontekstdə dövlətlərin müdafiə strategiyalarının adaptivliyi və informasiya təhlükəsizliyi sahəsində qabaqlayıcı tədbirlərin gücləndirilməsi xüsusi əhəmiyyət kəsb edir.

Süni intellekt (Aİ) və Big Data analitikası. Rəqəmsal informasiya mühitində *Big Data* (böyük həcmdə verilənlər) analitikası və sosial media platformalarındakı meyillərin izlənməsi müasir hibrid müharibənin əsas istiqamətlərindən birini təşkil edir. Süni intellekt və *machine learning* (maşın öyrənməsi) texnologiyaları dezinformasiyanın geniş yayılmasında, ictimai rəyə təsir edilməsində və müəyyən hədəf qruplarının manipulyasiyasında effektiv şəkildə istifadə olunur. Bu texnologiyalar vasitəsilə saxta xəbərlər və deepfake videolar avtomatik yaradılır, sosial media platformalarında müəyyən mövzular süni şəkildə trend halına gətirilir və ictimai fikir idarə olunur. Eyni zamanda *Big Data* analitikası kütləvi məlumat axınını emal edərək cəmiyyətin həssas nöqtələrini müəyyənləşdirir və bu zəifliklərdən istifadə edərək psixoloji təsir kampaniyaları təşkil etməyə imkan yaradır. Beləliklə, informasiya müharibəsinin yeni mərhələsi formalaşır və dövlətlərin milli təhlükəsizliyinə qarşı yönəlmiş qeyri-ənənəvi təhdidlər daha mürəkkəb və çətin aşkarlana bilən xarakter alır.

Deepfake texnologiyası. Süni intellektin inkişafı ilə vizual və səsli kontentin manipulyasiyası daha mürəkkəb və realistik hala gəlmişdir. Bu texnologiya vasitəsilə siyasi liderlərin, dövlət rəsmilərinin və ictimai fiqurların saxta video və audioları yaradılaraq onların mövqeləri təhrif edilir, ictimai rəyə təsir göstərilir və sosial sabitlik sarsıdılır. Deepfake texnologiyası təkcə siyasi manipulyasiya üçün deyil, həm də kiberfırıldaqçılıq, reputasiya hücumları (*reputation attacks*) və dezinformasiya kampaniyalarında geniş şəkildə istifadə edilir. Bu tip saxta kontentlər insanların şüuraltına təsir edərək onların emosional reaksiyalarını yönləndirir və cəmiyyətdə etimadsızlıq mühiti formalaşdırır. Bundan əlavə, deepfake texnologiyası sosial media platformalarında sürətlə yayılaraq real və saxta məlumatı bir-birindən ayırmağı çətinləşdirir, beləliklə, informasiya müharibəsində təsirli bir silaha çevrilir.

Sosial mühəndislik (social engineering). Sosial mühəndislik kibertəhlükəsizlik kontekstində mühüm rol oynayan və insanların psixoloji zəifliklərindən istifadə edərək dezinformasiyanın yayılmasına, məxfi məlumatların əldə edilməsinə və kiberhücumların effektiv şəkildə həyata keçirilməsinə yönəlmiş kompleks strategiyalardan ibarətdir. Hakerlər və kibercinayətkarlar dövlət qurumlarının, kritik infrastruktur obyektlərinin və ictimai rəyə təsir edən şəxslərin məlumatlarını sızdırmaq üçün bu texnikadan geniş istifadə edirlər. Onlar qurbanları aldadaraq konfidensial məlumatları

ələ keçirmək, zərərverici proqram təminatını sistemlərə yoluxdurmaq və təşkilatların daxili şəbəkələrinə qanunsuz giriş əldə etmək məqsədilə müxtəlif manipulyasiya üsullarına əl atırlar.

Sosial mühəndislik əsasən fişinq (phishing) hücumları, hədəfli dezinformasiya kampaniyaları və insan faktoruna əsaslanan texnikalar vasitəsilə həyata keçirilir. Bəzən kibercinayətkarlar qurbanları aldatmaq üçün saxta *e-poçt* və ya mesajlardan istifadə edir, bəzən isə müxtəlif ssenarilər quraraq onların etibarını qazanmağa çalışırlar. Süni intellekt texnologiyalarının inkişafı ilə bu hücumlar daha mürəkkəb və çətin aşkarlanan formalar almışdır. Bu səbəbdən dövlət və özəl qurumlar kibertəhlükəsizlik mövzusunda maarifləndirilməli, fərdi və təşkilati informasiya təhlükəsizliyi protokolları gücləndirilməli, real vaxt rejimində təhdidlərin aşkarlanmasına yönəlmiş qabaqlayıcı tədbirlər həyata keçirilməlidir.

Qabaqcıl dövlətlərin hibrid təhdidlərə qarşı mübarizə strategiyaları

Hibrid təhdidlərin artması dövlətlər üçün yeni müdafiə strategiyalarının qəbul edilməsini zəruri edir. Ölkələr bu təhlükələrə qarşı spesifik yanaşmalar tətbiq edir. Aşağıda qabaqcıl dövlətlərin bəzilərinin hibrid təhdidlərə qarşı həyata keçirdiyi tədbirlər təhlil edilir.

ABŞ. ABŞ hibrid təhdidlərə qarşı mübarizədə müxtəlif qabaqcıl texnologiya və metodlardan istifadə edir. Federal Təhqiqatlar Bürosu (FBI), Daxili Təhlükəsizlik Departamenti (DHS) və Müdafiə Departamenti (DoD) kimi qurumlar bu sahədə əsas rol oynayır. Bundan əlavə, ABŞ hibrid təhdidlərə qarşı Çoxmillətli Qabiliyyətlərin İnkişafı Koalisiyası (Multinational Capability Development Campaign – MCDC) çərçivəsində tərəfdaş ölkələrlə birgə strateji həllər üzərində çalışır. MCDC Amerika Birləşmiş Ştatlarının Birgə Qərargahlar İdarəsi **(**US Joint Staff**)** tərəfindən idarə olunan və 24 tərəfdaş ölkə ilə birgə həyata keçirilən çoxmillətli bir proqramdır [9]. Bu proqram hibrid müharibəyə qarşı strategiyaların hazırlanması, yeni hərbi və təhlükəsizlik konsepsiyalarının inkişaf etdirilməsi və gələcək təhlükələrə qarşı çevik cavab mexanizmlərinin formalaşdırılması məqsədini daşıyır.

ABŞ, həmçinin NATO və Avropa İttifaqı ölkələri ilə koordinasiyalı şəkildə hibrid təhdidlərə qarşı mübarizə strategiyalarını inkişaf etdirir**.** Hibrid Təhdidlərə Qarşı Avropa Mərkəzi **(**European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE**)** ilə birgə tədbirlər keçirir və bu mərkəz vasitəsilə transatlantik təhlükəsizlik sahəsində kritik infrastrukturun qorunması və informasiya təhlükəsizliyi sahəsində koordinasiyanı gücləndirir.

Kibertəhlükəsizlik və İnfrastruktur Təhlükəsizliyi Agentliyi (CISA) kritik infrastrukturun qorunması və kiberhücumların qarşısının alınması üçün xüsusi proqramlar həyata keçirir. Məsələn, CISA-nın "Einstein" adlı proqramı federal hökumət şəbəkələrində potensial təhdidləri aşkarlamaq və onlara qarşı tədbir görmək üçün hazırlanmışdır [10].

ABŞ hökuməti ilə özəl sektor arasında informasiya mübadiləsini gücləndirmək məqsədilə Məlumat Mübadiləsi və Təhlil Mərkəzləri (Information Sharing and Analysis Centers – ISACs) yaradılmışdır. Bu mərkəzlər vasitəsilə müxtəlif sektorlar kibertəhdidlər barədə məlumatları paylaşır və koordinasiyalı şəkildə cavab tədbirləri həyata keçirir.

Süni intellekt və maşın öyrənməsi texnologiyaları hibrid təhdidlərin aşkarlanması və qarşısının alınmasında mühüm rol oynayır. DHS böyük verilənləri *(Big Data)* təhlil edərək potensial təhdidləri erkən mərhələdə müəyyən edir. Məsələn, DHS-nin "Automated Indicator Sharing" (AIS) proqramı vasitəsilə kibertəhdid göstəriciləri real vaxt rejimində dövlət və özəl sektor arasında paylaşılır, bu da təhdidlərin sürətlə aşkarlanmasına və qarşısının alınmasına imkan yaradır [11].

Bundan əlavə, ABŞ hökuməti *"Cyber Storm"* kimi genişmiqyaslı kibertəlimlər keçirərək müxtəlif agentliklər və özəl sektor arasında koordinasiyanı təkmilləşdirir. Bu təlimlər real ssenarilər əsasında keçirilir və hibrid təhdidlərə qarşı hazırlığı artırır [12].

Ümumilikdə, ABŞ hibrid təhdidlərə qarşı mübarizədə texnoloji yeniliklərdən, "dövlət – özəl sektor əməkdaşlığı"ndan və proaktiv yanaşmalardan istifadə edərək milli təhlükəsizliyini qorumağa çalışır.

Böyük Britaniya. Böyük Britaniya hibrid təhdidlərə qarşı mübarizədə kompleks təhlükəsizlik strategiyası həyata keçirir və müxtəlif qurumlar vasitəsilə koordinasiyalı fəaliyyət göstərir. Ölkənin Müdafiə Nazirliyi (MoD) hibrid təhdidlərə qarşı qlobal mübarizə çərçivəsində Çoxmillətli Qabiliyyətlərin İnkişafı Koalisiyası (Multinational Capability Development Campaign – MCDC)

proqramında iştirak edir və onun inkişafına töhfə verir [13]. Bundan əlavə, Böyük Britaniya hökuməti Milli Kibertəhlükəsizlik Mərkəzi (National Cyber Security Centre – NCSC) vasitəsilə kritik infrastrukturun qorunması və kiberhücumların qarşısının alınması üçün tədbirlər həyata keçirir. NCSC dövlətlə özəl sektor arasında informasiya mübadiləsini təşviq edərək, kibertəhdidlərə qarşı kollektiv müdafiəni gücləndirir. Dezinformasiyaya qarşı mübarizə sahəsində hökumət Dezinformasiyaya Qarşı Mübarizə Bölməsi (Counter Disinformation Unit – CDU) vasitəsilə ictimaiyyəti yanlış məlumatlardan qorumaq üçün fəaliyyət göstərir. CDU, xüsusilə seçkilər və digər mühüm ictimai hadisələr zamanı dezinformasiyanın yayılmasının qarşısını almaq üçün tədbirlər görür.

Almaniya. Almaniya hibrid təhdidlərə qarşı institusional, qanunvericilik və texnoloji yanaşmaları birləşdirən strategiya həyata keçirir. Ölkənin əsas qurumları olan Federal İnformasiya Təhlükəsizliyi Ofisi (BSI) və Federal Konstitusiyanı Mühafizə Xidməti (BfV) kibertəhlükəsizliyin təmin edilməsi, dezinformasiyanın aşkarlanması və qarşısının alınması istiqamətində fəaliyyət göstərir. Bundan əlavə, Avropa İttifaqının Şərq Strateji Kommunikasiya İşçi Qrupu və NATO-nun Hibrid Təhdidlərə Qarşı Mərkəzi (Hybrid CoE) ilə əməkdaşlıq edərək xarici təsirlərin qarşısının alınmasına çalışır.

Almaniya hibrid müharibəyə qarşı mübarizədə qanunvericilik çərçivəsini genişləndirir və dezinformasiya əleyhinə müxtəlif hüquqi mexanizmlər tətbiq edir. Bu məqsədlə 2017-ci ildə qəbul edilmiş Şəbəkə Məcəlləsi Qanunu (NetzDG) sosial media platformaları qarşısında zərərli, təhqiredici və ya qanunvericiliyə zidd olan məzmunu silməyi vəzifə olaraq qoyur, əks halda, böyük cərimələr tətbiq edilir [14]. Bundan əlavə, Almaniya süni intellekt və *Big Data* analitikası vasitəsilə dezinformasiya kampaniyalarını və sosial mühəndislik texnikalarını aşkarlamaq üçün qabaqcıl texnologiyalardan istifadə edir.

Ölkə, həmçinin media savadlılığı və ictimai maarifləndirmə proqramlarını genişləndirməklə əhalini saxta xəbərlərə və kiberhücumlara qarşı hazırlayır. Federal Siyasi Maarifləndirmə Agentliyi **(**Bundeszentrale für politische Bildung – BPB**)** vasitəsilə dezinformasiyaya qarşı təhsil proqramları həyata keçirilir.

Ümumilikdə, Almaniya hibrid təhdidlərə qarşı milli təhlükəsizlik konsepsiyasını texnoloji innovasiya, qanunvericilik və beynəlxalq əməkdaşlıq ilə birləşdirən çoxvektorlu bir yanaşma tətbiq edir. Bu model təkcə kiberhücumlara və dezinformasiyaya qarşı deyil, eyni zamanda dövlət idarəçiliyinin müxtəlif səviyyələrində hibrid müharibə taktikalarına cavab verməyə imkan yaradır.

Çin. Çin hibrid təhdidlərə qarşı mübarizədə milli təhlükəsizlik konsepsiyasını genişləndirərək, kibertəhlükəsizlik və informasiya müharibəsinə qarşı sərt tədbirlər həyata keçirir. Dövlət Təhlükəsizlik Nazirliyi (Ministry of State Security – MSS) və Mərkəzi Hərbi Komissiya (Central Military Commission – CMC) bu sahədə əsas fəaliyyət göstərən qurumlardır.

Ölkə Böyük Çin Şəbəkə Təhlükəsizlik Divarı (*Great Firewall*) vasitəsilə informasiya axınına nəzarət edir və xarici dezinformasiyanın ölkə daxilində yayılmasının qarşısını almağa çalışır. Bundan əlavə, Milli Kibertəhlükəsizlik Strategiyası çərçivəsində kritik infrastrukturların qorunması və xarici təsirlərin məhdudlaşdırılması üçün xüsusi tədbirlər həyata keçirilir [15].

Süni intellekt və *Big Data* analitikası vasitəsilə yayılan informasiyaların izlənməsi, senzura və avtomatik moderasiya sistemlərinin tətbiqi Çin hökumətinin informasiya nəzarəti strategiyasının əsas elementlərindəndir. Həmçinin hökumət kibertəhlükəsizlik tədbirlərini gücləndirərək xarici aktorların ölkənin informasiya məkanına təsirini minimuma endirməyə çalışır.

Çin hibrid müharibə strategiyasını kiberkəşfiyyat və iqtisadi təsir vasitələri ilə dəstəkləyir. Çin Xalq Azadlıq Ordusunun Strateji Dəstək Qüvvələri (Strategic Support Force – SSF) və Çin Dövlət Təhlükəsizlik Nazirliyi (Ministry of State Security – MSS) kiber və informasiya əməliyyatları sahəsində fəaliyyət göstərərək dövlətin rəqəmsal mühitdə təsir gücünü artırır. APT41 və dövlət dəstəyi ilə fəaliyyət göstərən digər kiberqruplar MSS və SSF-in dəstəyi ilə kiberhücumlar və casusluq vasitəsilə xarici dövlətlərin hökumət sistemlərinə, kritik infrastrukturuna müdaxilə etməyə çalışır [16].

Bundan əlavə, Çin "Kəmər və Yol Təşəbbüsü" (Belt and Road Initiative – BRI) vasitəsilə qlobal iqtisadi təsir dairəsini genişləndirməyə çalışır. Bu təşəbbüs infrastruktur layihələri və strateji sərmayələr vasitəsilə digər ölkələrdə iqtisadi və siyasi nüfuzunu gücləndirmək məqsədini daşıyır [17].

Çin hökuməti texnoloji şirkətlərini hibrid strategiyaların tərkib hissəsi kimi istifadə edərək milli maraqlarını qorumaq və qlobal informasiya məkanında təsir gücünü artırmaq siyasəti yürüdür. Xüsusilə Huawei şirkəti hökumətlə yaxın əlaqələrinə görə Qərbin nəzarətinə məruz qalmış, ABŞ və müttəfiqləri onun 5G texnologiyalarından kibercasusluq üçün istifadə edə biləcəyini iddia edərək şirkəti dövlət infrastruktur layihələrindən kənarlaşdırmışdır. 2019-cu ildə Huawei "qara siyahıya" daxil edilərək ABŞ texnologiyalarına çıxışı məhdudlaşdırılmış, nəticədə şirkət öz mikroçip və proqram təminatı tədarük zəncirini yenidən qurmağa məcbur olmuşdur.

Ümumilikdə, Çin hibrid müharibə yanaşması ilə ənənəvi hərbi gücü qeyri-hərbi vasitələrlə birləşdirərək, münaqişələrdə kompleks və çoxşaxəli strategiya həyata keçirir. Bu model müxtəlif sahələrdə təsir imkanlarını genişləndirmək və rəqiblərə qarşı strateji üstünlük əldə etmək məqsədi daşıyır.

Rusiya. Rusiya hibrid müharibə strategiyalarını inkişaf etdirərək hərbi və qeyri-hərbi vasitələrin inteqrasiyasına xüsusi önəm verir. Bu yanaşma ənənəvi hərbi əməliyyatlarla yanaşı, informasiya müharibəsi, kiberəməliyyatlar və iqtisadi təsir kimi vasitələri də əhatə edir.

2013-cü ildə Rusiya Silahlı Qüvvələrinin Baş Qərargah rəisi Valeri Gerasimov müasir müharibələrin xarakterinin dəyişdiyini vurğulayaraq, hərbi və qeyri-hərbi vasitələrin birgə istifadəsinin vacibliyini qeyd etmişdir. Bu konsepsiya Qərbdə "Gerasimov Doktrinası" kimi tanınsa da, bəzi tədqiqatçılar bunu rəsmi doktrina kimi deyil, müasir müharibə üsullarına dair müşahidələr və ümumiləşdirmələr kimi qiymətləndirirlər [18].

Rusiya hibrid müharibə strategiyalarında qeyri-dövlət aktorlarından, xüsusilə də özəl hərbi şirkətlərdən geniş istifadə edir. Məsələn, "Vaqner" qrupu müxtəlif münaqişə bölgələrində fəaliyyət göstərərək təhlükəsizlik mühitinə təsir edir. Bu cür strukturların istifadəsi rəsmi hərbi iştirakın inkar edilməsinə və beynəlxalq reaksiyaların idarə olunmasına imkan yaradır [19].

Rusiya, həmçinin informasiya müharibəsi və strateji kommunikasiya vasitələrindən istifadə edərək ictimai rəyə təsir göstərir. Bu istiqamətdə müxtəlif media resursları, kiberəməliyyatlar və kommunikasiya strategiyalarından istifadə olunur. Belə metodlar, xüsusilə beynəlxalq münasibətlərdə və strateji maraqların təmin olunmasında effektiv vasitə kimi qiymətləndirilir. Bu yanaşmanın ən diqqətçəkən nümunələrindən biri 2014-cü ildə Krımın ilhaqı zamanı müşahidə olunmuşdur. Rusiya bu prosesdə ənənəvi hərbi güclə yanaşı, informasiya müharibəsi, siyasi manipulyasiya və yerli dəstək qruplarının mobilizasiyasını kombinə edərək hibrid müharibə strategiyalarını effektiv şəkildə tətbiq etmişdir. Bu prosesdə dezinformasiyanın yayılması, yerli ictimai rəyə təsir göstərilməsi və qeyri-müəyyənlik mühitinin yaradılması həlledici rol oynamışdır [20]. Eyni strategiya Ukraynanın şərqində, xüsusilə Donetsk və Luqansk bölgələrində də tətbiq olunmuş, separatçı qüvvələrin dəstəklənməsi və informasiya müharibəsi ilə hibrid münaqişə mühiti formalaşdırılmışdır. Həmin bölgələrdə qeyri-müəyyənlik və daxili qarşıdurmaların dərinləşdirilməsi, silahlı qrupların aktivləşdirilməsi və Rusiya mənşəli media platformaları vasitəsilə ictimai rəyə təsir göstərilməsi bu modelin əsas elementlərini təşkil etmişdir.

Bundan əlavə, Rusiya kiberəməliyyatları və informasiya müharibəsini xarici ölkələrdə siyasi proseslərə təsir göstərmək məqsədilə koordinasiyalı şəkildə tətbiq edir. Bunun ən bariz nümunəsi kimi 2016-cı il ABŞ prezident seçkiləri göstərilir. ABŞ kəşfiyyat xidmətlərinin hesabatlarına görə, Rusiyanın dövlət dəstəyi ilə hərəkət edən kiberqruplar və media platformaları sosial şəbəkələrdə koordinasiyalı dezinformasiya kampaniyaları həyata keçirmiş, ictimai rəyə təsir göstərmək üçün saxta xəbərlər və manipulyativ məzmun yaymışdır. Həmçinin kiberhücumlar vasitəsilə seçki ilə bağlı kritik məlumatların sızdırılması və seçki infrastrukturuna müdaxilə cəhdləri qeydə alınmışdır. Bu hadisə hibrid müharibənin siyasi təsir strategiyalarına nümunə kimi geniş şəkildə tədqiq edilmişdir [21].

Ümumiyyətlə, Rusiya hibrid müharibə yanaşması ilə ənənəvi hərbi gücü qeyri-hərbi vasitələrlə birləşdirərək, münaqişələrdə kompleks və çoxşaxəli strategiya həyata keçirir. Bu model müxtəlif sferalarda təsir imkanlarını genişləndirmək və rəqiblərə qarşı üstünlük əldə etmək məqsədi daşıyır.

Azərbaycanın hibrid təhdidlərə qarşı müdafiə strategiyası

Azərbaycan hibrid təhdidlərə qarşı mübarizə məqsədilə kompleks müdafiə strategiyası formalaşdırmışdır. Respublikamızın hibrid təhdidlər əleyhinə müdafiə strategiyasının əsas elementləri aşağıdakı kimi qruplaşdırıla bilər:

Milli təhlükəsizlik strategiyası

Azərbaycanın Milli Təhlükəsizlik strategiyası dövlətin suverenliyini və cəmiyyətin təhlükəsizliyini təmin etmək üçün həm daxili, həm də xarici səviyyədə kompleks tədbirlər sistemini ehtiva edir. Bu strategiyanın əsas hüquqi və konseptual çərçivəsini Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası və Hərbi Doktrina təşkil edir.

Milli Təhlükəsizlik Konsepsiyası milli maraqların qorunması üçün təhlükəsizlik siyasətinin əsas prinsiplərini müəyyən edir. Konsepsiyada vurğulandığı kimi, Azərbaycanın təhlükəsizlik mühitində mövcud qlobal və regional çağırışlara qarşı milli müdafiə mexanizmləri hazırlanmış və həyata keçirilmişdir [22]. Azərbaycanın təhlükəsizlik arxitekturası kibertəhlükəsizlik, dezinformasiyaya qarşı mübarizə, beynəlxalq əməkdaşlıq və sosial dayanıqlılıq kimi əsas elementlərin effektiv koordinasiyasına əsaslanır.

Azərbaycan Respublikasının Hərbi Doktrinası isə Milli Təhlükəsizlik Konsepsiyasının hərbi-strateji və hərbi-texniki əsaslarını inkişaf etdirir. Hərbi Doktrinanın 44-cü maddəsində qeyd olunduğu kimi, müasir təhlükəsizlik mühitində hərbi fəaliyyətlər yalnız genişmiqyaslı müharibələrlə məhdudlaşmır, onlar qeyri-nizami qüvvələr və informasiya-təbliğat kampaniyaları ilə birgə aparılaraq dövlətin təhlükəsizlik sisteminə təsir göstərə bilər. Eyni zamanda Hərbi Doktrinanın 42 və 46-cı maddələrinə əsasən, təhlükəsizlik mühitindəki qlobal və regional təhdidlərin dinamikasını izləmək və qabaqlayıcı tədbirlər görmək əsas prioritetlərdən biri hesab olunur [23]. Hərbi-strateji əsaslara görə, təhdidlərin vaxtında aşkarlanması, təhlili və qiymətləndirilməsi, habelə effektiv cavab mexanizmlərinin qurulması dövlətin təhlükəsizlik siyasətinin əsasını təşkil edir.

Milli təhlükəsizlik strategiyasında dövlətin müxtəlif sahələr üzrə müdafiə tədbirlərini əlaqələndirmək və genişmiqyaslı təhdidlərə qarşı sistemli yanaşma tətbiq etmək üçün hüquqi və icra mexanizmləri təsbit olunub. 2024-cü ilin sentyabr ayında Milli Məclisdə xarici müdaxilələrə və hibrid təhdidlərə qarşı xüsusi komissiyanın yaradılması bu istiqamətdə atılan mühüm addımlardan biridir. Komissiya ölkənin təhlükəsizliyini qorumaq, xarici təsirləri təhlil etmək və müvafiq qanunvericilik təklifləri hazırlamaq funksiyalarını yerinə yetirir. Onun fəaliyyəti Azərbaycanın müdafiə strategiyasında xüsusi yer tutur və dövlətin təhlükəsizlik tədbirlərini daha səmərəli və sistemli şəkildə həyata keçirməyə imkan yaradır [24].

Azərbaycanın təhlükəsizlik strategiyası beynəlxalq modellərlə müqayisədə özünəməxsus xüsusiyyətlərə malikdir. Xüsusilə Ermənistanla münaqişələr zəminində formalaşan bu strategiya ölkənin hibrid müdafiə mexanizmlərini inkişaf etdirməsinə şərait yaratmışdır. Müdafiə strategiyası beynəlxalq təcrübənin tətbiqi ilə yanaşı, regional ehtiyaclara uyğun lokal həllərin harmonik şəkildə birləşdirilməsi nəticəsində çevik və effektiv bir model kimi çıxış edir. Milli təhlükəsizlik strategiyası isə Milli Təhlükəsizlik Konsepsiyası və Hərbi Doktrinanın müəyyən etdiyi hüquqi və konseptual əsaslar çərçivəsində formalaşdırılmış, həm ənənəvi, həm də müasir təhlükələrə qarşı dayanıqlı bir müdafiə sisteminin yaradılmasını təmin etmişdir.

Kibertəhlükəsizlik

Hibrid təhdidlərin əsas istiqamətlərindən biri olan kiberhücumlar müasir təhlükəsizlik mühitində dövlətlərin milli maraqlarına ciddi təhdidlər yaradır. Azərbaycanda kiberhücumların yaratdığı təhlükələrin qarşısının alınması məqsədilə hüquqi, təşkilati, texnoloji və beynəlxalq səviyyədə genişmiqyaslı tədbirlər həyata keçirilmiş, eyni zamanda kibermənanın təhlükəsizliyinin təmin edilməsi üçün qanunvericilik bazası təkmilləşdirilmiş, müasir texnologiyalar tətbiq edilmiş, informasiya infrastrukturu gücləndirilmiş və beynəlxalq əməkdaşlıq genişləndirilmişdir. Bu tədbirlər kibertəhlükəsizlik sahəsində səmərəli müdafiə mexanizmlərinin qurulmasını təmin etmiş və hibrid təhdidlərin qarşısının alınmasında yüksək effektivliyə malik sistemlərin formalaşmasına şərait yaratmışdır.

Son illərdə Azərbaycana qarşı kiberhücumların sayı nəzərəçarpacaq dərəcədə artmışdır. Məsələn, 2020-ci ildə ölkəyə qarşı 2,2 milyon kiberhücum qeydə alınmışdır ki, bu da əvvəlki illərlə müqayisədə 2,6 dəfə çoxdur. Xüsusilə RDP protokolu (*Remote Desktop Protocol* – Microsoft tərəfindən inkişaf etdirilmiş və uzaqdan masaüstü idarəetmə üçün istifadə olunan protokol olub, bir kompüterin digər kompüterə uzaqdan qoşularaq onun ekranını idarə etməsinə imkan verir.) üzərindən həyata keçirilən bu hücumlar əsasən dövlət qurumları və infrastruktur obyektlərini hədəf almışdır [25]. 2022-ci ildə isə Azərbaycanın dövlət qurumlarına qarşı daha da intensivləşən kiberhücumlar müşahidə olunmuşdur. Elektron Təhlükəsizlik Xidmətinin məlumatına əsasən, bu dövrdə 48 saxta "gov.az" domeni bloklanmış, dövlət orqanlarına göndərilən 2 milyondan çox zərərverici və fişinq tərkibli e-poçtun qarşısı alınmışdır [26]. Bu faktlar Azərbaycanın kibertəhlükəsizlik sahəsində aktiv mübarizə apardığını və kritik dövlət infrastrukturlarının qorunması üçün effektiv tədbirlər gördüyünü göstərir.

İnformasiya təhlükəsizliyini təmin etmək məqsədilə qanunvericilik çərçivəsi gücləndirilərək "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" qanun qəbul edilmişdir [27]. Bu qanun informasiya təhlükəsizliyi və məlumatların qorunması üçün əsas prinsipləri müəyyən edir.

2009-cu ildə "Kibercinayətkarlıq haqqında" Konvensiyanı ratifikasiya etməklə, ölkə kibercinayətkarlığa qarşı mübarizə sahəsində beynəlxalq təcrübədən bəhrələnərək hüquqi və institusional çərçivəsini təkmilləşdirməyi, eləcə də qlobal təhlükəsizlik standartlarına inteqrasiyanı təmin etməyi qarşısına məqsəd qoymuşdur [28].

Kibertəhlükəsizliyin təmin olunmasında fərdi məlumatların qorunması xüsusi əhəmiyyət daşıyır. Bu məqsədlə qəbul edilmiş "Fərdi məlumatlar haqqında" qanun fərdi məlumatların toplanması, işlənməsi və məxfiliyinin təmin olunması qaydalarını tənzimləyir [29].

İnformasiya və kibertəhlükəsizliyin təmin olunmasında mühüm addımlardan biri 2023-cü ildə təsdiq edilmiş "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası"dır. Bu sənəd informasiya və kiberməkanın müdafiəsi ilə bağlı milli prioritetləri müəyyənləşdirir və strateji məqsədlərə nail olmaq üçün əsas fəaliyyət istiqamətlərini göstərir [30].

Azərbaycanda informasiya sistemlərinin qorunması və kiberhücumların qarşısının alınması üçün xüsusi qurumlar yaradılmışdır. Onlardan biri olan Elektron Təhlükəsizlik Xidməti kibertəhlükəsizlik sahəsində informasiya infrastrukturu subyektlərinin fəaliyyətinin koordinasiyasını həyata keçirir və cəmiyyəti mövcud elektron təhlükələr barədə məlumatlandırır [31]. Elektron Təhlükəsizlik Xidməti, həmçinin xarici tərəfdaşlarla, o cümlədən İsrailin "Technion" İnstitutu ilə əməkdaşlıq çərçivəsində təlim proqramları təşkil edir və kibertəhlükəsizlik üzrə təcrübə mübadiləsini gücləndirir. Bununla yanaşı, Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası (AKTA) kibertəhlükəsizliyi gücləndirmək və milli kiber potensialını inkişaf etdirmək məqsədilə həm yerli, həm də beynəlxalq səviyyədə kibertəhlükəsizlik qurumları və mütəxəssislərlə əməkdaşlıq edərək ölkədə kibermüdafiə mədəniyyətini inkişaf etdirir, maarifləndirmə və təlim proqramları təşkil edir [32].

Azərbaycanın kibertəhlükəsizlik sahəsində güclü və dayanıqlı müdafiə sistemlərini qurmaq əzmini əks etdirən bu hüquqi və təşkilati əsaslar hibrid təhdidlərə qarşı effektiv mübarizədə əhəmiyyətli rol oynayır.

İnformasiya təhlükəsizliyi və dezinformasiya ilə mübarizə

Azərbaycan Respublikasının milli təhlükəsizlik strategiyasında informasiya təhlükəsizliyi prioritet istiqamətlərdən biri kimi müəyyən edilmişdir. Son illərdə ölkəmiz əleyhinə aparılan dezinformasiya kampaniyaları bu sahədə kompleks mübarizə tədbirlərinin vacibliyini daha da aktuallaşdırmışdır. Xüsusilə 44 günlük Vətən müharibəsi dövründə və sonrakı mərhələdə yayılan manipulyativ məlumatlar informasiya təhlükəsizliyinin strateji əhəmiyyətini bir daha nümayiş etdirmişdir. Müharibə zamanı xarici media resurslarında və bəzi siyasi dairələrdə Azərbaycanın guya "suriyalı muzdlu döyüşçülərdən" istifadə etməsi və etnik təmizləmə siyasəti aparması barədə əsassız iddialar tirajlanmışdır [33]. Bu iddiaların hüquqi və faktiki heç bir sübutu olmamış, onların məqsədyönlü dezinformasiya kampaniyasının tərkib hissəsi olduğu müəyyən edilmişdir.

Bundan əlavə, 2024-cü ilin avqust ayında Azərbaycan ərazisində, guya, xarici hərbi qüvvələrin mövcudluğu barədə iddialar yayılmışdır [34]. Heç bir əsası olmayan bu informasiyanın məqsədli şəkildə ölkənin suverenliyini şübhə altına almağa xidmət etdiyi müəyyən edilmişdir. Eyni zamanda, Azərbaycanda keçirilən COP29 beynəlxalq konfransı ərəfəsində ölkə əleyhinə genişmiqyaslı dezinformasiya dalğası müşahidə olunmuşdur. Sammit zamanı müxtəlif platformalarda əsassız ittihamlar səsləndirilmiş, boykot çağırışları edilmiş, *süni intellekt* texnologiyalarından, o cümlədən deepfake metodlarından istifadə edərək Azərbaycan Respublikası Prezidentinin saxta videomüraciəti yayımlanmışdır. Bununla yanaşı, ölkənin ekoloji siyasətinə dair yanlış məlumatlar tirajlanaraq beynəlxalq ictimai rəyin manipulyasiya edilməsinə cəhd göstərilmişdir [35].

Sistemli şəkildə aparılan bu dezinformasiya kampaniyaları hibrid təhdidlərin bir hissəsi olmaqla, regionda sabitliyi pozmaq, beynəlxalq ictimai rəyi çaşdırmaq və Azərbaycanın strateji maraqlarına zərbə vurmaq məqsədi daşıyır. Bu tip hücumlar yalnız informasiyanı təhrif etməklə məhdudlaşmır, eyni zamanda siyasi, iqtisadi və diplomatik sahələrdə də təzyiq vasitəsi kimi istifadə olunur.

İnformasiya təhlükəsizliyinin təmin olunması və milli maraqların qorunması məqsədilə görülən hüquqi və praktiki tədbirlər mühüm əhəmiyyət kəsb edir. Bu sahədə Medianın İnkişafı Agentliyi jurnalistlərin peşəkar bacarıqlarını artırmaq, informasiya təhlükəsizliyini təmin etmək və dezinformasiyanın yayılmasının qarşısını almaq məqsədilə təlimlər təşkil edir. Agentlik ictimaiyyətin doğru məlumatla təmin olunmasına yönəlmiş fəaliyyətlər həyata keçirir [36].

Dövlət strukturları, media qurumları və vətəndaş cəmiyyəti institutlarının birgə səyləri ilə ölkədə informasiya təhlükəsizliyi və məlumat mühitinin etibarlılığı təmin olunur. Bütün bu tədbirlər Azərbaycanın informasiya təhlükəsizliyi sahəsində dayanıqlı bir sistem qurmaq istiqamətində olan əzmini və uğurlarını əks etdirir.

Beynəlxalq əməkdaşlıq

Hibrid təhdidlərə qarşı mübarizədə beynəlxalq əməkdaşlıqların rolu xüsusi əhəmiyyət kəsb edir. Azərbaycan NATO, Avropa İttifaqı, eləcə də digər beynəlxalq və regional təşkilatlarla sıx əməkdaşlıq edərək, məlumat mübadiləsi, təlim və təcrübə paylaşımı sahəsində mühüm imkanlardan yararlanır. Bu əməkdaşlıq ölkənin təhlükəsizlik infrastrukturunun gücləndirilməsində və hibrid təhdidlərə qarşı qabaqlayıcı tədbirlərin tətbiqində mühüm rol oynayır.

NATO ilə əməkdaşlıq çərçivəsində Azərbaycan kibertəhlükəsizlik, informasiya təhlükəsizliyi və hibrid təhdidlərə qarşı qabaqlayıcı tədbirlər sahəsində təcrübə əldə etmişdir. 1994-cü ildən NATO-nun "Sülh Naminə Tərəfdaşlıq" proqramına qoşulan Azərbaycan təhlükəsizlik sahəsindəki təlimlər və təcrübə mübadilələri ilə müdafiə imkanlarını genişləndirir. Bu əməkdaşlıq ölkənin təhlükəsizlik siyasətini inkişaf etdirmək və beynəlxalq standartlara uyğunlaşmaq baxımından mühüm əhəmiyyət kəsb edir.

Avropa İttifaqı ilə strateji tərəfdaşlıq, xüsusilə enerji və informasiya təhlükəsizliyi sahələrində Azərbaycanın müdafiə gücünü əhəmiyyətli dərəcədə artırır. Avropa İttifaqının "Şərq tərəfdaşlığı" proqramı çərçivəsində kibertəhlükəsizlik sahəsində qabaqcıl texnologiyaların tətbiqi Azərbaycanın təhlükəsizlik infrastrukturuna inteqrasiya edilir. Bu əməkdaşlıq dövlət qurumlarını kiberhücumlara qarşı daha davamlı etmək və ölkənin kibertəhlükəsizlik sahəsindəki təcrübəsini zənginləşdirmək məqsədi daşıyır.

Bundan əlavə, Azərbaycan BMT, ATƏT və MDB kimi beynəlxalq və regional təşkilatlarla təhlükəsizlik sahəsində əməkdaşlıq quraraq, hibrid təhdidlərə qarşı birgə tədbirlər həyata keçirir. Bu əlaqələr informasiya mübadiləsi və ortaq tədbirlər tətbiq etmək üçün vacib platforma yaradır. Beynəlxalq əməkdaşlıq çərçivəsində əldə olunan təcrübə və informasiya mübadiləsi Azərbaycanın hibrid təhdidlərə qarşı mübarizə strategiyasının effektivliyini artırır.

Azərbaycan kibertəhlükəsizlik sahəsində beynəlxalq əməkdaşlığın gücləndirilməsinə yalnız iştirakçı kimi deyil, həm də mühüm tədbirlərə ev sahibliyi etməklə töhfə verir. Bu istiqamətdə atılan addımlardan biri 2024-cü ilin sentyabr ayında Bakıda keçirilən 1-ci Beynəlxalq Kiberdiplomatiya Konfransı (ICCD – International Conference on Cyber Diplomacy) olmuşdur. Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin təşkilatçılığı ilə baş tutan tədbir kiberməkanın

təhlükəsizliyi və informasiya mübadiləsinin effektivliyinə yönəlmiş, konfrans çərçivəsində Kiberdiplomatiya üzrə Tərəfdaşlıq Mərkəzinin yaradılmasına dair Anlaşma Memorandumu imzalanmış və Bakı Bəyannaməsi qəbul edilmişdir [37].

İkitərəfli əməkdaşlıqlar da Azərbaycanın təhlükəsizlik sahəsindəki müstəqil gücünü artırır. İsrail və Türkiyə ilə kibertəhlükəsizlik texnologiyaları və mütəxəssis təlimləri sahəsində əməkdaşlıq Azərbaycan üçün əlavə təcrübə və resurslar təmin edir. Türkiyə ilə müdafiə sənayesi və Gürcüstan ilə strateji enerji layihələri sahəsindəki əməkdaşlıq Cənubi Qafqaz regionunda sabitlik və təhlükəsizliyin təminatında mühüm rol oynayır. Azərbaycan – Türkiyə – Gürcüstan üçtərəfli təhlükəsizlik platforması çərçivəsində həyata keçirilən layihələr regional sabitliyin qorunmasını təmin etməklə yanaşı, təhlükəsizlik sahəsində çoxtərəfli əməkdaşlıq modellərinin inkişafına imkan yaradır və qlobal təhlükəsizlik sisteminə inteqrasiyanı təşviq edir.

Bu cür çoxşaxəli əməkdaşlıqlar Azərbaycanın beynəlxalq nüfuzunu artırır, onu regionda və qlobal miqyasda təhlükəsizlik sahəsində etibarlı tərəfdaş kimi təqdim edir. Ölkənin hibrid təhdidlərə qarşı mövcud strategiyası yalnız milli təhlükəsizliyi deyil, həm də regional sabitliyi qorumağa xidmət edir.

Sosial təhlükəsizliyin təminatı və cəmiyyətin dayanıqlılığının gücləndirilməsi

Hibrid təhdidlərə qarşı mübarizə yalnız dövlət strukturlarının məsuliyyəti ilə məhdudlaşmır. Azərbaycanda cəmiyyətin bütün təbəqələrinin məlumatlandırılması və maarifləndirilməsi bu mübarizənin vacib hissəsidir. Görülən tədbirlər cəmiyyətin təhlükələrə qarşı müqavimətini artırmaq, sosial təhlükəsizliyi gücləndirmək və milli həmrəyliyi möhkəmləndirmək məqsədi daşıyır.

İnformasiya təhlükəsizliyinin təmin olunması və dezinformasiyaya qarşı mübarizə üçün ictimai kampaniyalar, fərdi təhsil proqramları və maarifləndirmə tədbirləri geniş tətbiq edilir. Bu yanaşma insanların tənqidi düşüncə bacarıqlarını inkişaf etdirərək, sosial mediada yayılan yanlış informasiyalara qarşı cəmiyyətin hazırlıqlı olmasını təmin edir. Bundan əlavə, kibertəhlükəsizlik və informasiya təhlükəsizliyi sahəsində ixtisaslı kadrların hazırlanması hibrid təhdidlərə qarşı müdafiə mexanizmlərinin gücləndirilməsində mühüm rol oynayır. Dövlət və cəmiyyətin qarşılıqlı fəaliyyəti, hibrid təhdidlərin müxtəlif formalarına qarşı dayanıqlı və effektiv müdafiə strategiyalarının formalaşdırılmasında mühüm rol oynayır.

Hibrid təhdidlərə qarşı müdafiə strategiyasının gücləndirilməsi üçün təkliflər

Müasir dövrün sürətli inkişaf dinamikası texnologiyaların, süni intellektin və rəqəmsal imkanların geniş yayılması ilə müşayiət olunur. Bu yeniliklər həyatın bir çox sahələrinə müsbət təsir göstərsə də, paralel olaraq yeni və daha mürəkkəb təhlükələrin yaranmasına səbəb olur. Xüsusilə kiberməkanın genişlənməsi və qlobal miqyasda rəqəmsal texnologiyaların təsir gücünün artması hibrid təhdidlərin daha mürəkkəb formalarının meydana çıxmasına şərait yaradır. Süni intellektin tətbiqi, *Big Data* analitikası və digər texnoloji yeniliklər bir tərəfdən dövlətlərə təhlükəsizlik sahəsində yeni imkanlar təqdim etsə də, digər tərəfdən qeyri-dövlət aktorlarının və düşmən qüvvələrin bu alətlərdən istifadəsini asanlaşdırır. Yeni reallıqlar milli təhlükəsizlik strategiyalarının həm çevikliyini, həm də effektivliyini təmin etmək üçün daha geniş spektrli üsulların tətbiqini tələb edir. Hibrid təhdidlərin çoxşaxəliliyini və onların milli, regional və qlobal təhlükəsizliyə təsirini nəzərə alaraq, mövcud resursların optimallaşdırılması, müasir həll yollarının tətbiqi və beynəlxalq əməkdaşlığın gücləndirilməsi zəruridir. Aşağıda bu sahədə həyata keçirilməsi məqsədəuyğun hesab edilən konkret təkliflər təqdim olunur:

1. **Kibertəhlükəsizlik və rəqəmsal müdafiə infrastrukturunun gücləndirilməsi**

– Dövlət və özəl sektor üçün kibertəhlükəsizlik standartlarının hazırlanması və tətbiqi (ABŞ və Böyük Britaniyanın dövlət-özəl əməkdaşlıq modellərinə əsaslanaraq).

– Davamlı monitorinq və qabaqlayıcı təhlükəsizlik yoxlamalarının genişləndirilməsi (İsrailin kiberhücumlara qarşı qabaqlayıcı analiz modellərindən istifadə edərək).

– Süni intellekt dəstəyi ilə dezinformasiyanın və deepfake texnologiyalarının aşkarlanmasına yönəlmiş sistemlərin inkişafı (Amerika Birləşmiş Ştatlarında DARPA-nın (Defense Advanced Research Projects Agency) “Media Forensics” (MediFor) proqramı və “Microsoft”un süni intellekt əsaslı

təhlükəsizlik həlləri, eləcə də Böyük Britaniyanın "National Cyber Security Centre" (NCSC) və "Alan Turing Institute"un deepfake aşkarlama sahəsindəki tədqiqatlarına əsaslanaraq).

– Kiberhücum simulyasiyalarının mütəmadi təşkili və qabaqlayıcı təlimlərin keçirilməsi (ABŞ və NATO ölkələrinin "red teaming" (Rəqib simulyasiyası) metodologiyalarından faydalanaraq).

– Kritik infrastrukturun kibertəhlükələrdən qorunması üçün milli müdafiə sistemlərinin gücləndirilməsi (Çinin tətbiq etdiyi "Great Firewall" modelindən seçilmiş yanaşmalar əsasında).

2. Dezinformasiyaya qarşı mübarizə və informasiya təhlükəsizliyinin təmin edilməsi

– Sosial media platformaları və media qurumları üçün tənzimləyici mexanizmlərin tətbiqi (Almaniyanın NetzDG qanununa uyğun modelin yaradılması ilə).

– Milli və beynəlxalq media savadlılığı proqramlarının tətbiqi və genişləndirilməsi (Böyük Britaniyanın media savadlılığı proqramlarına uyğun yanaşmaların inkişaf etdirilməsi ilə).

– İnformasiya müharibəsinə qarşı mütəxəssis qruplarının yaradılması və strateji kommunikasiya planlarının hazırlanması (Amerika Birləşmiş Ştatlarının "StratCom") modellərindən yararlanaraq).

– Dezinformasiyaya qarşı süni intellekt əsaslı analiz sistemlərinin qurulması (Amerika Birləşmiş Ştatlarının CISA və DARPA-nın "Semantic Forensics" (SemaFor) proqramı, eləcə də NATO-nun "StratCom" Mərkəzinin dezinformasiyanın aşkarlanması və qarşısının alınması üzrə tətbiq etdiyi metodlardan istifadə etməklə).

– Kritik informasiya mənbələrinin xarici təsirlərdən qorunması (Çinin xarici media təsirinə qarşı tətbiq etdiyi senzura və nəzarət metodlarından seçilmiş elementlər əsasında).

3. Hüquqi müdafiə və beynəlxalq əməkdaşlığın gücləndirilməsi

– Beynəlxalq hüquqi tədbirlərdə fəallığın artırılması və lobbiçilik fəaliyyətlərinin genişləndirilməsi (ABŞ və İsrailin beynəlxalq hüquqi lobbiçilik təcrübəsinə əsaslanaraq).

– "Lawfare" (hüquqi mübarizə) strategiyalarının tətbiqi və milli hüquqi mexanizmlərin gücləndirilməsi (Böyük Britaniya və Almaniyanın milli təhlükəsizlik strategiyalarına əsaslanaraq).

– Kibercinayətkarlığa qarşı milli qanunvericiliyin təkmilləşdirilməsi və hüquq-mühafizə orqanlarının bu sahədə bilik və bacarıqlarının artırılması.

– NATO, Avropa İttifaqı və MDB məkanında kibertəhlükəsizlik sahəsində əməkdaşlığın daha da genişləndirilməsi və çoxtərəfli müqavilələrin imzalanması.

4. Sosial dayanıqlılığın artırılması və milli həmrəyliyin gücləndirilməsi

– İnformasiya təhlükəsizliyi və milli təhlükəsizlik mövzusunda geniş maarifləndirmə proqramlarının təşkili (ABŞ və Böyük Britaniyanın "Digital Literacy" proqramlarına uyğun olaraq).

– İnformasiya müharibələrinin cəmiyyət üzərində yaratdığı psixoloji təsirlərin azaldılması üçün sosial və psixoloji dəstək proqramlarının həyata keçirilməsi.

– Milli həmrəyliyi gücləndirmək məqsədilə ictimai institutların rolunun artırılması və strateji kommunikasiya mexanizmlərinin inkişaf etdirilməsi.

Bu təkliflər Azərbaycanın hibrid təhdidlərə qarşı strateji davamlılığını artırmaqla yanaşı, milli təhlükəsizliyin təmin edilməsində çevik və dayanıqlı müdafiə mexanizmlərinin qurulmasını stimullaşdıraraq ölkənin daxili sabitliyini gücləndirməyə və Azərbaycanın beynəlxalq arenada etibarlı tərəfdaş kimi mövqeyini daha da möhkəmləndirməyə fokuslanmışdır. Qeyd olunan fəaliyyətlər, eyni zamanda regional və qlobal təhlükəsizlik mühitinə müsbət təsir göstərərək milli maraqların qorunmasını və strateji prioritetlərin həyata keçirilməsini təmin edəcək, Azərbaycanın təhlükəsizlik strategiyasını innovativ yanaşmalarla zənginləşdirəcək, müasir təhlükələrə qarşı dayanıqlı və adaptiv bir model kimi ölkəni hibrid təhdidlərə qarşı effektiv müdafiə edən unikal bir sistemə çevirəcəkdir.

Nəticə

Hibrid təhdidlər müasir beynəlxalq təhlükəsizlik sistemində dövlətlərin suverenliyinə, milli təhlükəsizliyinə və strateji maraqlarına qarşı yönəlmiş çoxşaxəli və kompleks təsir mexanizmlərindən ibarətdir. Bu təhdidlər informasiya manipulyasiyası, kiberhücumlar, iqtisadi təzyiqlər, hüquqi mexanizmlərin istifadəsi və vasitəçi qüvvələrin tətbiqi kimi müxtəlif üsullarla həyata keçirilir. Xüsusilə

süni intellekt texnologiyalarının inkişafı, deepfake və sosial mühəndislik metodlarının genişlənməsi hibrid müharibənin daha mürəkkəb və çətin aşkarlanan formalarını meydana çıxarmışdır.

Aparılan araşdırma göstərir ki, hibrid təhdidlərə qarşı mübarizədə bir sıra ölkələr uğurlu strategiyalar formalaşdırmışdır. İnformasiya təhlükəsizliyi, kibertəhlükəsizlik və hüquqi təzyiqlərə qarşı cavab tədbirlərinin sistemli şəkildə həyata keçirilməsi bu sahədə əsas yanaşmalardan biridir. Bu təcrübələr göstərir ki, qabaqlayıcı tədbirlər, strateji kommunikasiyanın gücləndirilməsi, milli kibermüdafiə sistemlərinin modernləşdirilməsi və informasiya müharibəsinə qarşı dayanıqlı mexanizmlərin qurulması hibrid hücumların qarşısının alınmasında mühüm rol oynayır.

44 günlük Vətən müharibəsində məğlub olan Ermənistan müharibə meydanında düçar olduğu uğursuzluqların əvəzi kimi, bəzi xarici tərəfdaşları ilə birlikdə informasiya və siyasi təzyiq vasitələrindən istifadə edərək mübarizəni yeni müstəviyə – hibrid müharibə müstəvisinə daşımağa çalışması müşahidə olunur. Xüsusilə beynəlxalq səviyyədə ölkəmizə qarşı müxtəlif platformalarda əsassız iddiaların yayılması, ekoloji məsələlər və insan hüquqları kimi mövzuların manipulyasiya edilməsi, deepfake texnologiyası ilə dövlət çaşçısını nüfuzdan salmaq məqsədi güdən saxta videomaterialların dövriyyəyə buraxılması, kiberhücumlar, hüquqi təzyiq (lawfare) və siyasi təzyiq cəhdləri hibrid hücumların bariz nümunəsidir. Bütün bunlar Azərbaycanın hibrid təhdidlərə qarşı mövcud müdafiə strategiyasını gücləndirmə ehtiyacını daha da aktuallaşdırmışdır.

Araşdırmada əldə olunan nəticələr sübut edir ki, ölkənin müdafiə konsepsiyası kibertəhlükəsizlik, dezinformasiyaya qarşı mübarizə, beynəlxalq əməkdaşlıq və cəmiyyətin dayanıqlılığının artırılması kimi əsas elementlərə söykənərək milli təhlükəsizlik sisteminin dayanıqlılığını təmin edir. Azərbaycan bu cür təhdidlərə qarşı hüquqi və diplomatik müstəvidə çevik cavab tədbirləri görərək beynəlxalq hüquq çərçivəsində öz maraqlarını qoruyur. Eyni zamanda regional təhlükəsizlik təşəbbüsləri və strateji tərəfdaşlıqlar vasitəsilə ölkənin müdafiə potensialı gücləndirilir. Gələcəkdə hibrid təhdidlərə qarşı strategiyanın effektivliyini daha da yüksəltmək üçün qabaqcıl texnologiyaların tətbiqi, milli hüquqi mexanizmlərin təkmilləşdirilməsi və beynəlxalq diplomatik əlaqələrin daha da gücləndirilməsi prioritet olaraq qalmalıdır.

İstifadə edilmiş ədəbiyyat siyahısı

1. Hoffman, F.G. Conflict in the 21st Century: The Rise of Hybrid Wars / F.G.Hoffman. – Arlington: Potomac Institute for Policy Studies, – 2007. – 10 p.

2. Milli Məclis. Xarici müdaxilələrə və hibrid təhdidlərə qarşı müvəqqəti komissiyanın yaradılması barədə qərar.: [Elektron resurs] / AZƏRTAC. – Bakı, 2024.
URL:https://azertag.az/xeber/milli_meclis_xarici_mudaxilelere_ve_hibrid_tehdidlere_qarsi_muveqqeti_komissiyanin_yaradilmasi_barede_qerar_layihesini_tesdiqleyib-3205570

3. Singer, P.W. Cybersecurity and Cyberwar: What Everyone Needs to Know / P.W.Singer, A.Friedman – Oxford: Oxford University Press, – 2014. – 21 p.

4. Jowett, G.S. Propaganda & Persuasion (6th ed.) / G.S.Jowett, V.O'Donnell – Thousand Oaks: Thousand Oaks: Sage Publications, – 2015. – 22 p.

5. Pomerantsev, P. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money / P.Pomerantsev, M.Weiss – New York: Institute of Modern Russia, – 2014. – 70 p.

6. Deshpande, V. (Ed.). Hybrid Warfare: The Changing Character of Conflict / V.Deshpande. – New Delhi: Pentagon Press, – 2021. – 122 p.

7. Kuçi, G. Russia's Hybrid Warfare in the Western Balkans: Geopolitical Strategies and Proxy Actors // – Berlin: Octopus Journal: Hybrid Warfare & Strategic Conflicts, – 2024. vol. 3, № 2, – s. 45: [Electronic resource] / URL: https://octopusinstitute.org/russias-hybrid-warfare-in-the-western-balkans

8. Murray, W., Mansoor, P.R. (Eds.). Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present // – Cambridge: Cambridge University Press, – 2012. – 90 p.

9. NATO. Multinational Capability Development Campaign (MCDC) –2023 Fact Sheet.: [Electronic resource] / – Norfolk, VA: NATO Allied Command Transformation, 2023.
URL: https://www.act.nato.int/wp-content/uploads/2023/05/2023_Fact_Sheet_MCDC.pdf?utm

10. Cybersecurity and Infrastructure Security Agency (CISA). EINSTEIN: National Cybersecurity Protection System.: [Electronic resource] / – Washington, DC: CISA, 2023.
URL: https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system/einstein?utm

11. Cybersecurity and Infrastructure Security Agency (CISA). Automated Indicator Sharing (AIS): Real-Time Cyber Threat Intelligence.: [Electronic resource] / – Washington, DC: CISA, 2023.
URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais?utm_source

12. Cybersecurity and Infrastructure Security Agency (CISA). Cyber Storm: National Cyber Exercise Series.: [Electronic resource] / – Washington, DC: CISA, 2023.
URL: https://www.cisa.gov/resources-tools/programs/cyber-storm

13. UK Ministry of Defence. Countering Hybrid Warfare: Multinational Capability Development Campaign (MCDC) Concepts & Considerations.: [Electronic resource] / – London: Ministry of Defence, 2019.
URL:https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf?utm

14. Bundesamt für Justiz (Federal Office of Justice, Germany). Guidelines on Regulatory Fines under the Network Enforcement Act (NetzDG).: [Electronic resource] / – Bonn: Bundesamt für Justiz, 2022.
URL:https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/NetzDG/Leitlinien_Geldbussen_en.pdf?__blob=publicationFile&v=3

15. The Friday Times. The Great Firewall: China's Security Strategies.: [Electronic resource] /
URL: https://thefridaytimes.com/19-Dec-2024/the-great-firewall-china-s-security-strategies

16. Mandiant. APT41: A Dual Espionage and Cyber Crime Operation.: [Electronic resource] / Mandiant. – 2022.
URL: https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf?utm

17. Ağalarlı, A., Əhmədov, E. Çinin Kəmər və Yol Təşəbbüsü: İqtisadi və Qeosiyasi Təsirlərin Təhlili. Metofizika, 8(1): [Elektron resurs] / – 2025.
URL: https://doi.org/10.33864/2617-751X.2025.v8.i1.225-237

18. Galeotti, M. On the Gerasimov Doctrine: Why the West Fails to Beat Russia to the Punch. / M.Galeotti. – Washington, DC: National Defense University Press, – 2019. – 252 p.

19. Singh, R. The Wagner Group: A Tool of Hybrid Warfare.: / R.Singh. – New Delhi: Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), – 2023. – 25 p.

20. Encyclopædia Britannica. Ukraine: The Poroshenko Administration.: [Electronic resource] /
URL: https://www.britannica.com/place/Ukraine/The-Poroshenko-administration

21. Office of the Director of National Intelligence. Assessing Russian Activities and Intentions in Recent US Elections // – ODNI: [Electronic resource] / – 2017.
URL: https://www.dni.gov/files/documents/ICA_2017_01.pdf

22. Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası // Azərbaycan Respublikası Prezidentinin 23 may 2007-ci il tarixli 2198 nömrəli Sərəncamı ilə təsdiq edilmişdir. [Elektron resurs] / – Bakı, 2007. URL: https://e-qanun.az/framework/13373

23. Azərbaycan Respublikasının hərbi doktrinası // Azərbaycan Respublikası Milli Məclisi tərəfindən 8 iyun 2010-cu il tarixdə qəbul edilmişdir. : [Elektron resurs] / – Bakı, – 2010.
URL: https://e-qanun.az/framework/19722

24. Azərtac. // Xarici Milli Məclis Xarici müdaxilələrə və hibrid təhdidlərə qarşı müvəqqəti komissiyanın yaradılması barədə qərar layihəsini təsdiqləyib.: [Elektron resurs] / – Bakı, 2024.
URL:https://azertag.az/xeber/milli_meclis_xarici_mudaxilelere_ve_hibrid_tehdidlere_qarsi_muveqqeti_komissiyanin_yaradilmasi_barede_qerar_layihesini_tesdiqleyib-3205570

25. Kiber hücumlar sərhəd tanımır.: [Elektron resurs] / – Bakı, 2024.
URL: https://vergiler.az/news/economy/11819.html?utm

26. Musayev, İ.: Azərbaycana kiberhücumların təşkili istiqamətləri bir çox hallarda qonşularımızı işarə edir.: [Elektron resurs] / – Bakı, 2024. URL: https://report.az/ikt/ilqar-musayev-azerbaycana-kiberhucumlarin-teskili-istiqametleri-bir-cox-hallarda-qonsularimizi-isare-edir/?utm
27. İnformasiya, İnformasiyalaşdırma və İnformasiyanın Mühafizəsi Haqqında Qanun // Azərbaycan Respublikasının Milli Məclisi tərəfindən 3 aprel 1998-ci il tarixində qəbul edilmişdir.: [Elektron resurs] / – Bakı, 1998. URL: https://e-qanun.az/framework/3525
28. Kibercinayətkarlıq Haqqında Konvensiya // Azərbaycan Respublikasının Prezidenti tərəfindən 30 aprel 2009-cu il tarixində təsdiq edilmişdir.: [Elektron resurs] / – Bakı, 2009. URL: https://e-qanun.az/framework/18619
29. Azərbaycan Respublikasının Fərdi Məlumatlar Haqqında Qanunu // Azərbaycan Respublikası Milli Məclisinin 11 may 2010-cu il tarixli 998-IIIQ nömrəli qərarı ilə qəbul edilmişdir.: [Elektron resurs] / – Bakı, 2010. URL: https://e-qanun.az/framework/19675
30. Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası // Azərbaycan Respublikası Prezidentinin 28 avqust 2023-cü il tarixli 4060 nömrəli Sərəncamı ilə təsdiq edilmişdir.: [Elektron resurs] / – Bakı, 2023. URL: https://e-qanun.az/framework/55045
31. Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidmətinin fəaliyyəti haqqında əsasnamə // Azərbaycan Respublikası Prezidentinin 5 mart 2013-cü il tarixli 833 nömrəli fərmanı ilə təsdiq edilmişdir.: [Elektron resurs] / – Bakı, 2013. URL: https://e-qanun.az/framework/25375
32. Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası. AKTA-nın Fəaliyyəti: [Elektron resurs] / AKTA. – Bakı, 2024. URL: https://www.akta.az
33. Xalq Qəzeti. Azərbaycan əleyhinə dezinformasiya yayanlar kimlərdir ?: [Elektron resurs] / – Bakı, URL: https://xalqqazeti.az/az/siyaset/195736-azerbaycan-eleyhine-dezinformasiya-yayanlar-kimlerdir?utm
34. 525-ci Qəzet. Azərbaycana qarşı dezinformasiya tirajlayanlar: [Elektron resurs] / – Bakı, 2024. URL: https://525.az/news/270189-azerbaycana-qarsi-dezinformasiya-tirajlayanlar?utm
35. Prezidentin adından yayılmış videomüraciət saxtadır: [Elektron resurs] / – Bakı, 2024. URL: https://qafqazinfo.az/news/detail/prezidentin-adindan-yayilmis-videomuraciet-saxtadir-415076
36. Media İnkişaf Agentliyinin rəsmi veb-saytı: [Elektron resurs] / – Bakı, 2024. URL: https://media.gov.az
37. Azərtac. Bakıda regionun ilk kiberdiplomatiya üzrə beynəlxalq konfransı keçirilib: [Elektron resurs] / – Bakı, 2024. URL:https://azertag.az/xeber/bakida_regionun_ilk_kiberdiplomatiya_uzre_beynelxalq_konfransi_kechirilib___yenilenib-3196870

Аннотация
Гибридные угрозы и стратегия обороны Азербайджана
Вугар Ширинов

В данной статье проводится анализ гибридных угроз, их сущности, рисков, которые они представляют для национальной безопасности, а также стратегий защиты, применяемых для их нейтрализации. В исследовании используется аналитический метод, что позволяет рассмотреть гибридные угрозы с различных аспектов и детально оценить их воздействие на национальную безопасность.

Гибридные угрозы представляют собой сочетание традиционных военных тактик с кибератаками, дезинформационными кампаниями, экономическим давлением, а также новейшими технологиями манипуляции, такими как искусственный интеллект и социальная инженерия, используемыми в качестве инструментов влияния на государства. В силу своего геополитического положения, энергетических ресурсов и региональных конфликтов Азербайджан относится к странам с высокой степенью подверженности гибридным угрозам. В

этом контексте в статье проводится всесторонний анализ комплексной стратегии противодействия гибридным угрозам, охватывающей политику национальной безопасности, меры по обеспечению кибербезопасности, противодействие дезинформации и возможности международного сотрудничества. Кроме того, исследуются модели защиты, реализуемые ведущими государствами, и выделяются элементы их практического применения, которые могут быть адаптированы для Азербайджана.

Ключевые слова: гибридные угрозы, оборонительная стратегия, национальная безопасность, кибербезопасность, международное сотрудничество, асимметричная война

Abstract

Hybrid threats and Azerbaijan's defense strategy

Vugar Shirinov

This article analyzes the nature of hybrid threats, which hold a significant position in the security environment of states, the risks they pose to national security, and the defense strategies employed to counter these threats. The study employs an analytical method, allowing for the examination of various aspects of hybrid threats separately and providing a comprehensive assessment of their impact on national security.

Hybrid threats incorporate not only conventional military tactics but also cyberattacks, disinformation campaigns, economic pressure mechanisms, as well as next-generation manipulation technologies such as artificial intelligence and social engineering, serving as instruments of influence against states. Due to its geopolitical position, energy resources, and regional conflicts, Azerbaijan is among the countries with a high risk of exposure to hybrid threats. In this context, the article is analysed detailed encompassing national security policies, cybersecurity measures, counter-disinformation efforts, and opportunities for international cooperation by using a comprehensive defence strategy against hybrid threats. Additionally, the study explores the defense models implemented by leading countries in response to hybrid threats and identifies aspects of these practices that could be applicable to Azerbaijan.

Keywords: hybrid threats, defense strategy, national security, cybersecurity, international cooperation, asymmetric warfare

Məqalə redaksiyaya daxil olmuşdur: 03.02.2025
Təkrar işlənməyə göndərilmişdir: 12.02.2025
Çapa qəbul edilmişdir: 11.03.2025