Pedaqoji Universitetin Xəbərləri. Humanitar, ictimai və pedaqoji-psixoloji elmlər seriyası –2021, C.69, №2, s. 58-69
Transactions of Pedagogical University. Series of humanitarian, social, pedagogical and psychological sciences – 2021, V.69, №2, pp. 58-69

İctimai elmlər

UOT 327.5

C.E.Əhmədli
Bakı Dövlət Universiteti
jeyhun.ahmadli9204@gmail.com

HİBRİD MÜHARİBƏ ALƏTLƏRİ VƏ YA HİBRİD TƏHDİDLƏRƏ KONKRET NÜMUNƏLƏR ƏSASINDA KONSEPTUAL BAXIŞ

Açar sözlər: *hibrid müharibə, hibrid təhdidlər, hibrid müharibə alətləri*

Müasir münaqişə və müharibələrin fundamental analizi onu göstərir ki, bəşəriyyət hibrid müharibə çağını yaşayır. Ayrı-ayrı ölkələrin öz rəqiblərinə (və ya düşmənlərinə) qarşı açıq hibrid müharibə strategiyası həyata keçirdiyi müşahidə olunmaqdadır. Hətta bəzi ölkələr artıq özünün hərbi doktrina və təhlükəsizlik konsepsiyalarına hibrid təhdidlərlə bağlı xüsusi müddəalar daxil etmişdir. Hibrid müharibə zamanı istifadə olunan alətlər isə sonsuz saydadır. Lakin elə alətlər var ki, onlar demək olar ki, bütün müasir münaqişələrdə özünü göstərməkdədir. Bu alətlərə informasiya hücumları, kiber müdaxilələr, hədəf ölkələrdə terrorçu təşkilatların maliyyələşdirilməsi, siyasi partiya və ayrı-ayrı təşkilatlara sponsorluq edilməsi, özəl (muzdlu) hərbi birləşmələrin köməyindən faydalanmaq, iqtisadi təzyiqlər, çirkli təbliğat və s. daxildir. Məqalənin yazılmasında məqsəd adıçəkilən hibrid müharibə alətlərinin müasir münaqişə və ya müharibələrdə tətbiqini göstərməkdir.

Дж.Э.Ахмедли

СРЕДСТВА ГИБРИДНОЙ ВОЙНЫ ИЛИ КОНЦЕПТУАЛЬНЫЙ ОБЗОР ГИБРИДНЫХ УГРОЗ НА КОНКРЕТНЫХ ПРИМЕРАХ

Ключевые слова: *гибридная война, гибридные угрозы, инструменты гибридной войны*

Фундаментальный анализ современных конфликтов и войн показывает, что человечество живет во времена гибридных войн. Замечено, что некоторые страны используют стратегию открытой гибридной войны против своих соперников (или врагов). Некоторые страны даже включили специальные положения о гибридных угрозах в свои военные доктрины и концепции безопасности. Инструменты, используемые в гибридной войне, безграничны. Однако есть инструменты, которые проявляются практически во всех современных конфликтах. К ним относятся информационные атаки, кибератаки, финансирование террористических организаций, спонсирование политических партий и отдельных организаций в целевых странах, использование частных (наемных) воинских формирований, экономическое давление, грязная

пропаганда и так далее. Цель написания этой статьи – показать применение этих инструментов гибридной войны в современных конфликтах или войнах.

J.E.Ahmedli

MEANS OF HYBRID WAR OR A CONCEPTUAL OVERVIEW OF HYBRID THREATS ON SPECIFIC EXAMPLES

Keywords: *hybrid warfare, hybrid threats, hybrid warfare tools*

A fundamental analysis of modern conflicts and wars shows that humanity is living in a time of hybrid warfare. It is observed that some countries have an open hybrid war strategy against their rivals (or enemies). Some countries have even included special provisions on hybrid threats in their military doctrines and security concepts. The tools used in hybrid warfare are endless. However, there are tools that are manifested in almost all modern conflicts. These include information attacks, cyber-attacks, financing terrorist organizations, sponsoring political parties and individual organizations in target countries, use of private (mercenary) military units, economic pressure, dirty propaganda, and so on. The purpose of writing this article is to show the application of these hybrid warfare tools in modern conflicts or wars.

Yeni nəsil müharibələri xarakterizə etmək üçün indiyə qədər bir neçə termindən istifadə olunmuşdur. Bəzi elmi araşdırmalarda asimmetrik müharibə, IV nəsil müharibə, qarışıq müharibə (“compound wars”), sərhədsiz müharibə (“unrestricted wars”), təmassız müharibə (“contactless war”) və s. terminlər diqqəti cəlb edir. 2014-cü ildə Krımın anneksiyası və Ukraynanın şərqində alovlanmış separatizm Qərbdəki siyasi və akademik dairələr tərəfindən müasir müharibələrin daha dərindən və konseptual şəkildə öyrənilməsinə səbəb olmuşdur. Həmin vaxtdan etibarən yeni nəsil müharibələrin ümumi məcmusu elmi ədəbiyyatlarda “hibrid müharibə” kimi adlandırılmağa başlayıb.

Təxminən 10 ildir bu mövzuda qəbul olunan bütün beynəlxalq hüquqi-siyasi sənədlərdə “hibrid müharibə”, “hibrid təhdid” terminlərindən istifadə edilir. 2011-ci ildə NATO komandanlığının hazırladığı hesabatda hibrid təhdid “terrorizm, miqrasiya, piratçılıq, korrupsiya, etnik toqquşma və digər düşmən fəaliyyətləri əhatə edən termin” kimi xarakterizə olunmuşdur [32, s.77-98]. Həmin hesabatda vurğulanır ki, hibrid müharibə elementləri keçmişdə olduğu kimi situativ deyil, sistemli və çoxşaxəli formada həyata keçirilən strategiyadır. Hesabatın müvafiq hissəsində bu cümlə olduğu kimi öz əksini tapır: “Hibrid təhdidlər düşmənlər tərəfindən uzun vədəli siyasi hədəfləri gerçəkləşdirmək üçün istifadə olunur”. NATO-nun keçmiş baş katibi Andres Foq Rasmussen Rusiyanın Ukraynada həyata keçirdiyi kampaniyanı açıq hibrid müharibə kimi dəyərləndirmiş və baş verən prosesləri belə özətləmişdir: Rusiya Ukraynadakı yeni hökuməti zəiflətmək və Şərqi Ukraynada Rusiyanın siyasi təsirini davam

etdirmək məqsədilə hərbi əməliyyatlara paralel olaraq müxtəlif gizli fəaliyyətlər və geniş dezinformasiya kampaniyasını eyni anda aparır [20]. ABŞ Müdafiə Nazirliyinin 2006-cı və 2010-cu illərdə yayımladığı 4 illik hesabatda keçmiş müdafiə naziri Robert Geitsin çıxışlarında hibrid təhdidlərdən bəhs olunmuşdur.

Hibrid təhdidlər elmi ədəbiyyatlarda həm də hibrid müharibə alətləri kimi öyrənilir. Tarixi aspektlərdən yanaşdıqda bu alətlərin bir qisminin əslində tarixin ən müxtəlif dövrlərində bu və ya digər şəkildə istifadə olunduğunu görə bilərik. Elm və texnologiyanın sürətli inkişafı həmin alətlərin zamanla təkmilləşərək müasir forma və məzmun kəsb etməsini şərtləndirmişdir. Bu mənada bəzi hibrid müharibə alətlərinin yeni olmadığını irəli sürə bilərik, lakin bütövlükdə hibrid müharibənin əsas səciyyəvi xüsusiyyəti heç də alətlərin yeniliyi ilə yox, onların birləşərək yaratmış olduğu effektlə xarakterizə edilir. Böyük Britaniya Müdafiə Nazirliyinin hibrid təhdidlərə qarşı qlobal mübarizə məqsədilə təşəbbüs etdiyi MCDC proqramının 2017-ci il hesabatında qeyd edilir ki, hibrid müharibə asimmetrikdir və üfüqi, şaquli ox boyunca çoxsaylı güc alətlərindən istifadəni nəzərdə tutur. Hesabatda qeyd olunur ki, hibrid müharibə aktoru effektiv nəticə əldə etmək üçün bir və ya daha çox aləti intensiv tətbiq edə (şaquli yüksəlmə) və ya bir çox alətin təsir imkanlarını eyni anda sinxronlaşdıra (üfüqi yüksəlmə) bilər [21, s.8]. Daha sadə ifadə etsək, ən müxtəlif alət və vasitələr ortaq bir siyasi hədəf uğrunda eyni anda tətbiq olunduğu təqdirdə hibrid müharibə meydana gəlir. Lakin elə alətlər də vardır ki, onlar hibrid müharibənin sütununu təşkil edir və demək olar ki, hibrid müharibə aparan əksər ölkələr tərəfindən istifadə olunmaqdadır. Həmin alətlər barədə tədqiqat aparılmışdır.

Təcrübələr onu göstərir ki, hibrid müharibə aparan ölkənin ən çox müraciət etdiyi vasitələrdən biri rəqib (düşmən) ölkədə ictimai şüura təsir etmək məqsədilə ayrı-ayrı təşkilatların fəaliyyətinə dəstək olmaqdır. Qlobal geosiyasi ambisiyalara sahib olan bəzi ölkələr xaricdə öz maraqlarına uyğun fikirləri təbliğ edən təşkilat və ya düşüncə mərkəzlərini maliyyələşdirməyə çalışır, ya da təməldən bu cür təşkilatlara sponsorluq edirlər. Rusiya və Çinin bu metoddan istifadə etdiyini bir çox nümunələrdə görə bilərik. Məsələn, 2015-ci ildə Pekinin maliyyə dəstəyi ilə ABŞ-da Çin-Amerika Elmləri İnstitutu yaradıldı. Siyasi analitiklər hesab edir ki, bu elmi-tədqiqat mərkəzinin yaradılmasında əsas məqsəd ABŞ-da Çinlə bağlı müsbət təsəvvürlər aşılamaqdır [16].

Eyni qaydada Rusiya da Avropada bir sıra təşkilat və partiyalara sponsorluq etməklə həm özü ilə bağlı müsbət imic formalaşdırmağa çalışır, həm də bu təşkilatlardan ayrı-ayrı ölkələrin hakimiyyətlərinə qarşı təsir aləti kimi istifadə edir. 2006-cı ildə Rusiya dövləti xarici ölkələrdəki təşkilatları arasında kommunikasiyanı təmin etmək məqsədilə Dünya Ruslarının Koordinasiya Şurasını təsis etdi. 2016-cı ildə Berlində əsası qoyulan və rusiyalı biznesmenlərin maliyyəsi ilə fəaliyyət göstərdiyi iddia olunan Sivilizasiyaların

Dialoqu Araşdırma İnstitutu Rusiya dövlətinə bağlılığını təkzib etsə də, öz fəaliyyətində Rusiyanın maraqlarından çıxış etdiyini gizlədə bilmir. Almaniyanın "Frankfurter Allgemeine Zeitung" qəzeti həmin təşkilatı "Moskvanın hibrid müharibə aləti" kimi təsvir edib [10]. Rusiyanın Avropada maliyyələşdirdiyi beyin mərkəzlərinin əsas fəaliyyət istiqaməti Moskvanın yürütdüyü qlobal siyasətin Avropa xalqlarının mənafeyinə cavab verdiyi reallığını təbliğ etməkdir. Məsələn, Rusiyanın Strateji Tədqiqatlar İnstitutunun Avropada yerləşən ofisləri uzun illər Monteneqro və İsveçin NATO ilə yaxşınlaşmasını önləmək məqsədilə geniş təbliğat işi aparmış və bu ölkələrin NATO-ya üzv olmasının heç bir müsbət perspektiv vəd etmədiyi fikrini formalaşdırmağa çalışmışdır [27].

Eyni alətdən istifadə edərək hibrid müharibə strategiyasının qurulması ABŞ üçün də səciyyəvidir. Belə ki, dünyanın dörd bir yanında demokratiya və insan hüquqlarına dəstək adı altında ayrı-ayrı qeyri-hökumət təşkilatlarına maliyyə donorluğu etməsi bu reallığı aydın şəkildə üzə çıxarır. Araşdırmalar onu göstərir ki, həm Soros, həm də onun Açıq Cəmiyyət Vəqfləri dünyada 200-dən çox ABŞ təşkilatını birbaşa, yaxud da dolayı yolla maliyyə ilə təmin edir [34]. Bütün fəaliyyətində ABŞ-ın milli maraqlarından çıxış edən Soros vəqfləri elə bu amilə görə Rusiya elmi-siyasi dairələri tərəfindən Amerikan imperializminin təsirli alətlərindən biri kimi təsvir olunur. Rusiyalı analitiklər hesab edir ki, Soros fondu "milli dövlət" anlayışını aradan qaldırmaqla ABŞ-ın öncüllüyü ilə qlobal supergücün formalaşması məqsədinə xidmət edir [5].

Hibrid müharibə aparan ölkələrin xaricdə maliyyələşdirdiyi əsas təsisatlardan biri də siyasi partiyalardır. Xüsusən, Avropa ölkələrində Rusiya ilə yaxınlığı ilə seçilən bir sıra siyasi partiyaların Kremldən maliyyələşdiyi haqqında xeyli iddialar irəli sürülmüşdür. Latviyada fəaliyyət göstərən Harmoniya Mərkəzi partiyasının, Estoniyada isə Mərkəz Partiyasının Moskvadan maliyyələşdiyi haqqında ciddi şübhələrin olduğu irəli sürülmüşdür [8, s.20]. Eyni qaydada Fransada Marin le Penin ultra-sağçı Milli Cəbhə partiyasının 2017-ci il prezident seçkiləri ərəfəsində Rusiya banklarından kreditlər aldığı iddia olunmuşdur [24]. Adıçəkilən siyasi partiyaların fəaliyyətində diqqət cəlb edən əsas xüsus liberal dəyərlərə qarşı olması, anti-Amerikan və anti-Qərb baxışları ilə seçilməsidir. Siyasi partiyaların maliyyələşdirilərək hibrid müharibə aləti kimi istifadə olunması Qərb dövlətləri üçün də xasdır. Məsələn, Ermənistanın hazırda hakimiyyətdə olan "Mənim addımım" siyasi blokunun Qərb fondlarından maliyyə dəstəyi aldığına dair ciddi iddialar irəli sürülmüşdür. Qeyd olunur ki, Soros fondu 1997-2008-ci illər arasında hazırkı baş nazir Nikol Paşinyanın rəhbərlik etdiyi siyasi təşkilatlara 48 milyon dollar yardım etmişdir [10]. Azərbaycan Respublikasının Prezidenti İlham Əliyevin 2020-ci ilin oktyabrında "TASS" agentliyinə müsahibəsində Paşinyanı "Sorosun əlaltısı" adlandırması bu baxımdan diqqəti cəlb edir [1].

Ümumiyyətlə, son illər dünyada populyarlıq qazanmış "narıncı inqilablar" dalğasının arxasında müxalif siyasi partiyaların ABŞ və bir sıra Avropa ölkələri tərəfindən maliyyələşdirildiyi faktının olması şübhə doğurmur.

Düşmən (rəqib) ölkələrdə etiraz mitinqlərinin təşkil olunması hibrid müharibənin ən effektiv alətlərindən biri hesab edilir. Kremlin Avropada təşkil etdiyi küçə nümayişlərini buraya daxil edə bilərik. Məsələn, 2017-ci ildə Hollandiyada Ukrayna ilə ticarətə dair keçirilmiş referendumun nəticələrinə təsir göstərmək məqsədilə Moskva anti-Avropa İttifaqı meyilli qrupların etiraz mitinqlərini təşkil etməyə nail oldu [14]. Ehtimal olunur ki, Rusiya həm də Bolqarıstanda şist qazın istifadəsinə qarşı çıxan qrupların etiraz nümayişinə dəstək göstərmişdir. Bu da o məqsəddən irəli gəlir ki, Bolqarıstan hökuməti Qərbdə üstünlük verilən şist qaz istifadəsi fikrindən daşınsın və dolayısilə Bolqarıstanın Rusiya təbii qazından asılılığı bundan sonra da davam etsin [12]. Qeyd edək ki, bu etirazlar Bolqarıstan baş naziri Boyko Borisovun şist qazın kəşfiyyatını aparmaq üçün "Chevron" şirkətinə verilmiş lisenziyanı ləğv etməsi ilə nəticələndi. 2011-ci ildən etibarən dünyada böyük əks-səda yaratmış "Ərəb baharı" hərəkatının ABŞ və bir sıra qərb dövlətləri tərəfindən təşkil olunduğu heç kəsə sirr deyil. O baxımdan ki, ABŞ-ın o vaxtkı prezidenti Barak Obama həmin inqilabi prosesi açıq şəkildə dəstəklədiyini ifadə etmişdir [18]. Yeri gəlmişkən qeyd etmək lazımdır ki, Rusiyanın hibrid təhdidlərə qarşı mübarizə strategiyasının əsasını təşkil edən Gerasimov doktrinası "Ərəb baharı"ndan təsirlənmişdir.

Hibrid müharibə aləti kimi istifadə olunan metodlardan biri də oliqarxların nüfuzundan və maliyyə imkanlarından faydalanmaqdır. Bu daha çox Rusiyanın tətbiq etdiyi mexanizmlərdən biridir. Moskva hər zaman xarici ölkələrdə siyasət, kommersiya, media və ticarət əlaqələri olan Rus oliqarxları ilə təmaslarını möhkəm saxlayır. Bu oliqarxlar yerli qurumlarla sıx əlaqələr saxlayır, lazım olduqda isə öz sahələrindəki nüfuz və imkanlarından istifadə edərək siyasi proseslərə Kremlin müəyyən etdiyi istiqamətlər üzrə təsir göstərirlər. Məsələn, Rus-Yunan əsilli iş adamı İvan Savvidisin Yunanıstan iqtisadiyyatında çox böyük yatırımları mövcuddur. Savvidis həm də Yunanıstanın televiziya və media sektorunda önəmli paylara sahibdir. O, ötən müddət ərzində əlində olan resurslardan istifadə edərək Yunanıstandakı Qərbyönümlü siyasi qüvvələrə qarşı təbliğat işi aparmışdır [7, s.7-8]. Rusiya bu texnologiyadan Ukraynada daha geniş tətbiq etmişdir. Hətta Vladimir Zelenski prezident seçildikdən sonra Ukraynada Rusiya meyilli oliqarxlara qarşı sanksiyalar da həyata keçirməyə cəhd etmişdir [33].

Müşahidələr onu göstərir ki, varlı oliqarxlardan hibrid müharibə aləti kimi istifadə etmək daha çox Rusiyanın müraciət etdiyi təcrübə olub. Lakin elə hibrid müharibə alətləri də vardır ki, onlardan daha çox ABŞ başda olmaqla bir sıra Qərb ölkələri, eyni zamanda İran daha çox faydalanmışdır. Söhbət məzhəb

və ya təriqətlərdən, o cümlədən ayrı-ayrı etnoslardan proksi güc vasitəsi kimi istifadədən gedir. ABŞ Orta Şərqdə öz geosiyasi maraqlarını reallaşdırmaq, xüsusən İranı blokada şəraitində saxlamaq üçün təkcə sünni məzhəbinə məxsus dövlətlərlə müttəfiqlik münasibəti qurmaqla kifayətlənməmiş, həm də sünni mərkəzli qanunsuz silahlı birləşmələri maliyyə və zəruri silah-sursatlarla təmin etmişdir. Vaşinqton bu məqsədini reallaşdırmaq üçün ayrı-ayrı etnoslara xüsusi rəğbətini də heç vaxt gizlətməmişdir. Dünyanın bir çox ölkələri tərəfindən terrorçu təşkilat kimi tanınan Suriyadakı PKK-PYD silahlı birləşmələrinin ABŞ tərəfindən aşkar sürətdə dəstəklənməsi İran və Rusiyanın bölgədəki fəallığından duyulan narahatlıqlarla bağlıdır [2]. Təkcə 2020-ci ildə ABŞ sözügedən təşkilata 400 milyon dollarlıq dəstək proqramı həyata keçirmişdir [3]. Ziddiyyətli məqam ondan ibarətdir ki, ABŞ rəsmi şəkildə İran, Suriya, Şimali Koreya və Kubanı terrorizmi maliyyələşdirən ölkələr kimi tanımasına baxmayaraq özü müttəfiqi Türkiyənin terrorçu təşkilat kimi tanıdığı qanunsuz silahlı birləşmələri dəstəkləməkdən çəkinməmişdir. Bu, bir tərəfdən ikili standartlı yanaşma kimi diqqəti cəlb edirsə, digər tərəfdən, ABŞ-ın həyata keçirdiyi hibrid müharibə strategiyasının mürəkkəb kombinasiyalara malik olmasından xəbər verir.

İran idarəçilik fəlsəfəsi baxımından teokratik ölkə olduğuna görə məzhəb faktorundan öz rəqibləri ilə müqayisədə daha effektiv güc vasitəsi kimi istifadə edə bilir. Rəsmi Tehranın aşkar sürətdə dəstəklədiyi şiə mərkəzli "Hezbullah" təşkilatı Orta Şərq coğrafiyasında ən təsirli proksi güc alətlərindən biri hesab olunur. İran məhz həmin təşkilat vasitəsilə regionda şiə koridoru yaratmaq kimi əsas strateji məqsədini reallaşdırmağa çalışır. İddialara görə, "Hezbullah"ın təkcə Suriya ərazisindəki fəaliyyətini təşkil etmək üçün İran tərəfindən hər il 50-100 milyon dollar vəsait ayrılır [16, s.1].

Hibrid müharibə alətləri içərisində ən müasir və geniş tətbiq olunanlar arasında kiber əməliyyatların xüsusi yeri vardır. Ümumiyyətlə, kiber əməliyyatlar riski az, maliyyəsi aşağı olsa da, effektiv nəticələri kifayət qədər yüksəkdir. Bu, kiber alətləri yoxsul və ya iqtisadi göstəriciləri aşağı olan ölkələr üçün daha cəlbedici edir. Bu gün dünyada demək olar ki, əksər ölkələr, o cümlədən, ABŞ, Rusiya, Çin kimi supergüclər də kiber hücumlara məruz qalırlar. Rusiya Federal Təhlükəsizlik Xidmətinin (FSB) açıqladığı məlumatlara görə, təkcə 2016-cı ildə Rusiya dövlətinin ayrı-ayrı təsisatlarına ümumilikdə 70 milyon kiber hücum təşkil olunmuşdur [6]. Ümumiyyətlə, kiber fəza üç formada istismar edilir: casusluq, hücum və manipulyasiya [36]. Kiber casusluq məzmun etibarilə ənənəvi casusluğa çox yaxındır və hibrid müharibə aparan ölkə üçün zəruri məlumatları toplamağı nəzərdə tutur. Bu cür məlumatlar hibrid müharibə aparan ölkələr tərəfindən ya ictimailəşdirilir (süni şəkildə rəy formalaşdırmaq məqsədilə), ya da məxfi saxlanılmaqla müxtəlif məqsədlər üçün istifadə edilir. Məsələn, "APT 28" və "APT 29" Rusiya kəşfiyyat

xidmətinə bağlı dünyaca məşhur haker qruplarıdır və xarici ölkələrdə kiber casusluq etməkdə peşəkarlaşmışdır [35]. Kod adı qeyd olunmuş həmin haker qruplarının ABŞ-da Dövlət Departamenti, Ağ Ev və digər dövlət agentliklərinə casusluq məqsədilə çoxsaylı hücumları təşkil olunmuşdur [30]. Rusiyaya bağlı haker qrupları ABŞ-da 2016-cı il prezident seçkilərinin gedişatına süni yollarla ciddi təsir göstərməkdə ittiham edilirlər [28]. Həyata keçirilən haker müdaxilələrinin 2016-cı il seçkilərinin nəticələrinə birbaşa təsiri hələ tam aydınlaşmasa da (baxmayaraq ki, ABŞ kəşfiyyatının gəldiyi qənaətə görə, kiber müaxilələrin səslərin hesablanmasına heç bir təsiri olmamışdır), ehtimal olunur ki, Rusiya dövlətinin əsas məqsədi ABŞ-dakı seçki sisteminin zəif tərəfləri ilə bağlı material və zəruri məlumatlar əldə etməkdir ki, gələcəkdə bu ölkəyə qarşı kiber müstəvidə daha effektiv hibrid müharibə apara bilsin. Bu da nəzəri olaraq kiber casusluğun əsas məqsədi kimi dəyərləndirilə bilər.

Kiber fəzada aparılan müharibənin digər bir forması kiber hücumlardır. 2010-cu ildə İranın komputer şəbəkələrində "Stuxnet" adlı zərərverici proqramın aşkar olunması yeni bir kiber müharibə texnikasının yaranmasına gətirib çıxardı. Dünyanın ilk rəqəmsal silahı hesab olunan "Stuxnet" digər zərərli haker proqramlarından fərqli olaraq, təkcə informasiyanı oğurlamaqla kifayətlənməyib, həm də kompüterlərin nəzarət etdiyi fiziki avadanlıqları məhv edirdi [8]. Qərbdən təşkil olunmuş bu haker hücumlarının əsas məqsədi İranın nüvə proqramına xəsarət yetirmək idi. "Stuxnet" dövlətlərin milli təhlükəsizliyi baxımından böyük dilemma yaratdı. Bu, ilk növbədə kiber alətlərin fiziki müstəvidə ağır zərər vura bilmə qabiliyyəti ilə bağlıdır. Kiber hücumlar xüsusən 2007-ci ildə Estoniyada strateji infrastrukturu hədəf alaraq ağır böhrana səbəb oldu. Tallinin mərkəzində bir Sovet abidəsinin dağıdılmasına cavab olaraq hakerlər Estoniyanın demək olar ki, bütün elektron infrastrukturunu – əsas ticarət banklarını, telekampaniyalarını, mediya qurumlarını və serverlərini iflic etdilər [20].

Kiber müdaxilələrin üçüncü forması kiber manipulyasiyalarıdır. Haker qrupları bir sistemə giriş əldə etdikdən sonra komputer şəbəkəsində saxlanan məlumatları idarə etmək və ya dəyişdirmək istəyə bilərlər. 2015-ci ildə ABŞ Milli Təhlükəsizlik Agentliyinin direktoru Maykl Rogers ifadə etmişdir ki, informasiya manipulyasiyaları gələcəkdə çox böyük problemlərə yol açа bilər. Ən ciddi elektron manipulyasiya insidentlərindən biri 2013-cü ildə Suriyalı hakerlərin "Assosiated Press" agentliyinin rəsmi Tvitter hesabını sındıraraq həmin media qurumunun adından Ağ Evdə partlayışın olduğu, Barak Obamanın isə yaralandığı barədə feyk məlumat paylaşılan zaman yaşanmışdır. "Bloomberg"in verdiyi məlumata görə, bu insident nəticəsində "Dow Jones" indeksi 150 ballıq enişi etdi, dünya səhm bazarı isə 136 milyard dollarlıq itki ilə üzləşdi [20]. Siyasi məqsədlər üçün məlumatları manipulyasiya etmək üçün ilk cəhdlərdən biri 2016-cı ildə ABŞ prezident seçkiləri zamanı yaşandı. Həmin

vaxt İllinoys ştatının seçicilər bazasına giriş əldə etmiş rus hakerlər qeydiyyatdan keçən şəxslərin məlumatlarını dəyişdirməyə cəhd etmişdilər, lakin bu, uğursuzluqla nəticələnmişdir [23]. Təcrübələr onu göstərir ki, məlumat sabotajı (və ya kiber manipulyasiya) potensial dağıdıcı təsirləri nəzərə alınmaqla digər iki kiber təhdid formasından daha ağır nəticələrə səbəb ola bilər.

Təsirli hibrid müharibə alətlərindən biri də iqtisadi amillər üzərindən təzyiq siyasətidir. Hər nə qədər yeni vasitə olmasa da, müasir dövrdə ən vacib və təsirli rıçaqlardan biri hesab olunur. Birləşmiş Ştatlar uzun müddətdir ki, bu alətdən ən effektiv istifadə edən ölkə kimi diqqəti cəlb edir. Qloballaşma prosesinin də təsiri ilə iqtisadi təzyiq alətlərinin effektivliyini əhəmiyyətli dərəcədə artırmışdır. ABŞ-ın rəhbərliyi ilə bir sıra Qərb ölkələri artıq 10 illiklərdir ki, liberal dəyərlər arxasında gizlətdikləri geosiyasi maraqları naminə Rusiyaya qarşı iqtisadi sanksiyalar tətbiq etməkdədirlər. Qərbin Rusiyaya qarşı ən genişmiqyaslı iqtisadi sanksiyası Ukrayna böhranının yaşandığı dövrə təsadüf edir. O sanksiyaların bir çoxu hələ də qüvvəsindədir. Sanksiyalar gözlənildiyi kimi, Rusiya rublunun çökməsinə və Rusiya maliyyə böhranına səbəb oldu [31]. Maraqlı məqam odur ki, Rusiyaya qarşı tətbiq olunan iqtisadi sanksiyalar Rusiyadan çox Qərbin özünə ciddi zərər vurmuş oldu. Belə ki, 2015-ci ilədək Avropa ölkələri bu sanksiyalara görə 100 milyard avro itki ilə üzləşdi [25]. Rusiya Maliyyə Nazirliyinin açıqlamasına görə isə 2014-cü il ərzində tətbiq olunan sanksiyaların Rusiya iqtisadiyyatına vurduğu zərərin ümumi məbləği 40 milyard avro təşkil edir [15]. Rusiya Prezidenti Vladimir Putin isə ABŞ-ın Səudiyyə Ərəbistanı ilə birlikdə dünya neft bazarındakı qiymətləri də qəsdən süni şəkildə aşağı endirdiklərini bildirmişdir [4]. 2016-cı ilin ortalarına qədər sanksiyalardan dolayı Rusiya iqtisadiyyatının üzləşmiş olduğu zərərin məbləği 170 milyard dollardır. Həmin dövr ərzində neft-qaz qiymətlərindəki düşüşə görə Rusiya 400 milyard dollar itirmişdir [29]. Rusiya Prezidentinin yuxarıda qeyd olunan bəyanatından çıxış etsək, Ukrayna hadisələrinə görə Qərbin tətbiq etdiyi iqtisadi sanksiyalar təkcə 2016-cı ilə qədər Rusiya iqtisadiyyatına 570 milyard dollar zərər vurmuşdur. Digər tərəfdən isə Qərb dövlətlərinin özünün bu sanksiyalara görə üzləşdiyi itkiləri nəzərə alsaq, iqtisadi sanksiyaların hibrid müharibə aləti kimi ən maliyyətli vasitə olduğunu deyə bilərik. Sanksiyaların effektivliyini dəyərləndirsək, bəzi analitiklər hesab edir ki, sanksiyalar Kremlin Ukrayna ilə bağlı siyasətinin dəyişməsinə, habelə Rusiyanın bölgədəki hərbi aktivliyinin qismən zəifləməsinə səbəb olmuşdur [19]. Ukraynanın o vaxtkı prezidenti Pyotr Poroşenko isə sanksiyaları "Rusiyanı aqressiv siyasətdən çəkindirəcək əsas faktorlardan biri" kimi dəyərləndirmişdi [26].

Çin də artan iqtisadi gücündən beynəlxalq məsələlərdə təsir mənbəyi kimi istifadə edir. ABŞ-a məxsus THAAD raketdən müdafiə komplekslərinin

Cənubi Koreyada yerləşdirilməsi Pekinin öz qonşusuna qarşı bir sıra iqtisadi sanksiyalar tətbiq etməyə vadar etdi. Çindən Cənubi Koreyaya turist səfərlərinə qadağalar qoyuldu, Cənubi Koreya məhsulları boykot edildi. Nəticədə Çin və Cənubi Koreya Prezidentlərinin 2017-ci ildə keçirilmiş görüşündə razılıq əldə olunur ki, Seul ABŞ-la hərbi müttəfiqliyi məhdudlaşdırmaq barədə öhdəlik götürür, bunun müqabilində isə sanksiyalar aradan qaldırılır [13]. Beləliklə, Çin bir dənə güllə atmadan ABŞ raketdən müdafiə komplekslərinin öz qonşuluğundan çıxarılmasına nail olur.

Təəssüf ki, Ermənistan dövləti ölkəmizə qarşı apardığı təcavüz siyasətində həm də hibrid müharibə təhdidlərindən geniş istifadə etmişdir. İşğal dövründə Ermənistan tərəfdən həm ölkəmizin informasiya məkanına mütəmadi hücumlar təşkil olunmuş, çoxsaylı kibercinayətlər törədilmiş, həm də xaricdəki erməni şəbəkələri tərəfindən Azərbaycanın beynəlxalq imicinin korlanmasına hesablanan çirkli təbliğat siyasəti həyata keçirilmişdir. Ermənistan dövləti apardığı işğalçılıq siyasətini ört-basdır etmək üçün dezinformasiya oyunu təşkil edərək dünya ictimaiyyətini aldatmağa cəhd etmişdir. Lakin düşmənin informasiya təhdidlərinə qarşı həyata keçirdiyimiz sistemli mübarizə bu mənfur niyyətin baş tutmamasını şərtləndirmişdir. Ermənistan terrorçu təşkilatları açıq şəkildə dəstəkləyən, onları maliyyələşdirərək öz məqsədləri naminə istifadə edən bir ölkədir. Qarabağ döyüşlərində Ermənistan tərəfdən çoxsaylı terrorçuların vuruşması aşkar hibrid müharibə nümunəsidir. Ümumiyyətlə, İrəvan Orta Şərqdə əməkdaşlıq etdiyi terrorçu birləşmələrin köməyindən həm birinci, həm də ikinci Qarabağ müharibəsində faydalanmışdır.

ƏDƏBİYYAT

1. İlham Əliyev Rusiyanın TASS informasiya agentliyinə videomüsahibə verib.19 oktyabr 2020-ci il / https://president.az/articles/43547
2. ABD'nin YPG ısrarının perde arkası, Ali Çınar, 22 fevral 2021 / https://www.milliyet.com.tr/yazarlar/ali-cinar/abdnin-ypg-israrinin-perde-arkasi-6437530
3. ABD'den terör örgütü YPG/PKK'ya 400 milyon dolarlık destek, 03.10.2020 / https://www.aa.com.tr/tr/dunya/abdden-teror-orgutu-ypg-pkkya-400-milyon-dolarlik-destek/1994279
4. Владимир Путин: мы сильнее, потому что правы / https://tass.ru/top-officials/1589319
5. Многополярность и открытое общество: геополитический реализм против космополитической утопии. Pluriversum vs Universum, 30.10.2019 / https://www.geopolitica.ru/article/mnogopolyarnost-i-otkrytoe-obshchestvo-geopoliticheskiy-realizm-protiv kosmopoliticheskoy
6. ФСБ: около 70 млн. кибератак было совершено на российские объекты в течение года. 24 января, 2017 / https://russian.rt.com/world/news/353071-

fsb-kiberataki-na-rossiyskie-obiekti

7. *Alina Polyakova and others.* The Kremlin's Trojan Horses 2.0: Russian Influence in Greece, Italy, and Spain, Atlantic Council, November 2017 / https://www.atlanticcouncil.org/wp-content/uploads/2017/11/The_Kremlins_Trojan_Horses_2_web_1121.pdf
8. *Andrew Radin.* Hybrid Warfare in the Baltics: Threats and Potential Responses. Santa Monica, CA: RAND Corporation, 2017 / https://www.rand.org/pubs/research_reports/RR1577.html
9. An Unprecedented Look at Stuxnet, the World's First Digital Weapon by Kim Zetter. 11.03.2014 / https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
10. Armenia is a country controlled by Soros Foundation, 05 october, 2020 / https://news.ru/en/business/armenian-russian-economic-relations-unilateral-benefit/
11. *Ben Knight*. "Putin associate opens Russia-friendly think tank in Berlin" Deutsche Welle, July 1, 2016 / https://www.dw.com/en/putin-associate-opens-russia-friendly-think-tank-in-berlin/a-19372110
12. Bulgarians see Russian hand in anti-shale protests. 30 nov. 2014 / https://www.ft.com/content/e011d3f6-6507-11e4-ab2d-00144feabdc0
13. China wins its war against South Korea's US THAAD missile shield – without firing a shot, David Josef Volodzko, 18 Nov., 2017 / https://www.scmp.com/week-asia/geopolitics/article/2120452/china-wins-its-war-against-south-koreas-us-thaad-missile
14. *Christopher S.* Chivvis, "Understanding Russian "Hybrid Warfare": And What Can Be Done About It" / https://www.rand.org/pubs/testimonies/CT468.html
15. Finance Minister: oil slump, sanctions cost Russia $140 billion a year, Smith, Geoffrey. November 24, 2014 / https://fortune.com/2014/11/24/finance-minister-oil-slump-sanctions-cost-russia-140-billion-a-year/
16. Hezbollah: The Model of a Hybrid Threat, Bulletin, The Polish İnstitute of İnternational Affairs, 2 march 2015 / https://www.files.ethz.ch/isn/188946/Bulletin%20PISM%20no%2024%20(756)%202%20March%202015.pdf
17. *Isaac Stone Fish*. "Beijing Establishes a D.C. Think Tank, and No One Notices," Foreign Policy, July 7, 2016 / https://foreignpolicy.com/2016/07/07/beijing-establishes-washington-dc-think-tank-south-china-sea/
18. Islamism, the Arab Spring and the Failure of America's Do-Nothing Policy in the Middle East. October 9, 2015 / https://www.theatlantic.com/international/archive/2015/10/middle-east-egypt-us-policy/409537/
19. Is it time for Europe to excuse Russia's aggression? by Liubov Nepop, 25 september 2015 / https://www.euractiv.com/section/europe-s-east/opinion/is-it-time-for-europe-to-excuse-russia-s-aggression/
20. *Joshua Davis*. Hackers Take Down the Most Wired Country in Europe, Wired, August 21, 2007 / https://www.wired.com/2007/08/ff-estonia/

21. *Mark Landler, Michael R. Gordon*, "NATO Chief Warns of Duplicity by Putin on Ukraine", The New York Times, 8 iyul 2014 / https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html
22. MCDC Countering Hybrid Warfare Project, Understanding Hybrid Warfare, 2017 / https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf
23. *Michael Riley and Jordan Robertson*. Russian Cyber Hacks on U.S. Electoral System Far Wider than Previously Known, June 13, 2017 / http://cs.brown.edu/people/jsavage/VotingProject/2017_06_13_Bloomberg_RussianCyberHacksOnUSElectoralSystem.pdf
24. National Front seeks Russian cash for election fight, by İvo Oliviero, 2016 / https://www.politico.eu/article/le-pen-russia-crimea-putin-money-bank-national-front-seeks-russian-cash-for-election-fight/
25. Newswalk: Sleep Scientist Russell Foster on How He Stopped Seeing Life in Black and White, Sharkov, Damien (19 June 2015) / https://www.newsweek.com/newswalk-sleep-scientist-russell-foster-how-he-stopped-seeing-life-black-and-328999
26. Poroshenko: Sanctions, heroism of our warriors are key elements to overcome Russian aggression, 03.09.2015 / http://www.nrcu.gov.ua/en/news.html?newsID=6022
27. Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security / https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf
28. Report of the select Committee on intelligence United States Senate on Russian active measures campaigns and interference in the 2016 US election, Volume 1: Russian efforts against eletion infrastructure with additional views / https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf
29. Russia loses $600 billion on sanctions and low oil prices, Trude Pettersen / https://thebarentsobserver.com/ru/node/414
30. Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce, By Ellen Nakashima and Craig Timberg, Dec. 14, 2020 / https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
31. Russia's rouble crisis poses threat to nine countries relying on remittances, 18 January 2015 / https://www.theguardian.com/world/2015/jan/18/russia-rouble-threat-nine-countries-remittances
32. *Sascha-Dominik Bachmann, Hakan Gunneriusson*, Hybrid Wars: The 21st Century's New Threats to Global Peace And Security", Scientia Militaria - South African Journal of Military Studies, Vol. 43, Num. 1, 20 may 2015

33. Ukraine's Sanctions Against Pro-Russian Oligarch Medvedchuk - All About Oil and Coal, by Alla Hurska, February 24, 2021 / https://jamestown.org/program/ukraines-sanctions-against-pro-russian-oligarch-medvedchuk-all-about-oil-and-coal/
34. US organisations sponsored by Soros, 2017 / https://www.geopolitica.ru/en/article/us-organisation-sponsored-soros
35. What to know about the Russia-linked hackers accused of stealing COVID vaccine data, 16 July 2020 / https://abcnews.go.com/International/russia-linked-hackers-accused-stealing-covid-vaccine-data/story?id=71819152
36. WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents. New York Times, March 7, 2017 / https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html?_r=0

Redaksiyaya daxil olub 20.04.2021