**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН**

**MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN**

Қазақстан Республикасы Ақпарат және Қоғамдық Даму Министрлігі
Министерство Информации и Общественного Развития Республики Казахстан
Ministry of Information and Public Development of the Republic of Kazakhstan

# «ЖАЛПЫ ҒЫЛЫМ МЕН БІЛІМНІҢ ЖАРШЫСЫ»

## Республикалық ғылыми журналы

## Republican Scientific Journal

# "BULLETIN OF UNIVERSAL SCIENCE AND EDUCATION"

## Республиканский научный журнал

# «ВЕСТНИК ВСЕОБЩЕЙ НАУКИ И ОБРАЗОВАНИЯ»

***№ 6(1)2024***

***«ЖАЛПЫ ҒЫЛЫМ МЕН БІЛІМНІҢ ЖАРШЫСЫ»***
***Республикалық ғылыми журналы***

***Республиканский научный журнал***
***«ВЕСТНИК ВСЕОБЩЕЙ НАУКИ И ОБРАЗОВАНИЯ»***

***№6(1)2024***

**ISSN 2791-3449**

*«ЖАЛПЫ ҒЫЛЫМ МЕН БІЛІМНІҢ ЖАРШЫСЫ» Республикалық ғылыми журналы. – Астана: Қазақстан Республикасы ақпарат және қоғамдық даму министірлігі 2024 – 258 бет.*

*Республиканский научный журнал «ВЕСТНИК ВСЕОБЩЕЙ НАУКИ И ОБРАЗОВАНИЯ» - Астана: Министерство информации и общественного развития Республики Казахстан 2024. – 258 с.*

**ISSN 2791-3449**



Мерзімді баспасөзбасылымының ақпараттық агенттігі және желілікбасылымды қайта есепкеалу туралы КУӘЛІК
№ KZ83VPY00026374,
Астана қаласы

СВИДЕТЕЛЬСТВО
№ KZ83VPY00026374 город Астана
о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания

ӘОЖ 327.5

**[1]Амирбек А., [2]Нәзірқұл А.**
[1]PhD доцент, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Қазақстан,Түркістан.
[2]Қожа Ахмет Ясауи атындағы Халықаралық қазақ–түрік уиверситеті,Қазақстан,Түркістан.
E–mail: E-mail: aidarbek.amirbek@ayu.edu.kz

# ГИБРИДТІК ҚАУІП-ҚАТЕРЛЕР МЕН СОҒЫСТЫҢ НЕГІЗГІ ЭЛЕМЕНТТЕРІ

***Аңдатпа***

*XXI ғасыр жаһандану дәуірімен сипатталатыны белгілі. Осы тұрғыда барша адамзат бір бірімен тығыз қарым қатынас орнатады. Барша адамзат бұл ғасырды жаһандық ынтымақтастықтың жаңа дәуірі ретінде үміт артқан болатын. Бірақ та бұл ғасыр саяси қайшылықтарға толы болып, қауіпсіздіктің барлық түрінде сипат алып көрінінс табады. Халықаралық қатынастардың қазіргі кезеңі қарсыласпен ұрыс алаңында күш сынасып, оны етіп жеңу үшін стратегиялар мен тактикалар құрып, жеңіске жету секілді стандартты соғыс жүргізу тактикаларының маңыздылығының азаюымен ерекшеленіп отыр. Қазір мемлекеттің әскери күш-қуаты оның қуаттылығының негізгі факторынан сол елдің ақпараттық, экономикалық, саяси, мәдени, демографиялық, қаржылық мүмкіндіктері сияқты факторларға деңгейлес факторлардың біріне айналуда. Осылайша мемлекеттердің мәселелерді тек әскери күшпен шешу мүмкіндігі азайып, оларға соғыс майдандарында жаңа қосымша ресурстарды яғни алуан түрлі гибридті стратегияларды қолдану мәжбүрлігі туындады. Қазіргі әлемдегі «жұмсақ күш» тактикалары мен технологияларын қолдану туралы сөз бастамас бұрын, аталған терминге қатысы бар ұғымдар мен терминдердің мағынасына қысқаша тоқталған жөн. Сонымен ғылыми қауымдастықта «гибридті соғыс» ұғымына өлімге алып келетін мемлекеттер арасындағы қарулы (әскер, жеке әскери компаниялар, көтерілісші жасақтарын қолдану арқылы жүзеге асатын) қақтығыстармен қатар қарсыласқа дипломатиялық және экономикалық қысым көрсету, «түрлі-түсті революциялар» ұйымдастыру, киберқауіп төндіру, хакерлік шабуылдар мен тыңшылық әрекеттер жасау және ықтимал қарсыласқа қысым көрсету мақсатында қолайлы ақпараттық кеңістік құру секілді бейбіт ықпал ету құралдарын қолдану да жатады. Шынында, мемлекет пайдалана алатын гибридті соғыстың бейбіт кезеңіне «жұмсақ күш» стратегиясын қолдану жатады. Ойындар теориясының басым бөлігі дамыған мемлекеттердің позициясына қарай жүруде. Әлемдегі болып жатырған ойындар теориясының ауыспалы болуы гибридті қауіп қатерлердің пайда бола отырып, үлкен және кішілі соғыстардың сонымен қатар жұмсақ күштің белгілерінің артып, мемлекеттердің гибридті соғыс элементтерін білуді міндеттейді. Әр мемлекет гибридті қауіп қатерлермен күрес жүргізбес бұрын, оның негізгі элементтерін айқындайды. Әлемдегі мемлекеттер гибридті қауіппен өзінше күреседі. Алдағы уақытта мемлекеттер гибридті қауіп қатерді тіпті байқамай қалуы мүмкін,себебі ол әр түрлі жағдайда орын алуы мүмкін. Осы орайда, гибридті қауіптің негізгі элементтерін тарихи сахнаға енгеніне көп болмаған Орталық Азия мемлекеттерінің шеңберінде зерттеу қажеттілігі туды.*

***Кілттік сөздер:*** *Орталық Азия, гибридті қауіп, жұмсақ күш, Қытай, Батыс мемлекеттері, соғыс,Еуропалық Одақ, түрлі түсті революция*

**Кіріспе**

1980 жылы Джозеф Най «жұмсақ күш» терминін анықтап, оның үш құрамдас бөлігін айқындайды: елдің мәдениеті, құндылықтары және саяси идеологиясы мен сыртқы саясаты. Ал қазіргі кезде ақпараттық технологиялар мен медиа кеңістіктің белсенді дамуына байланысты, мемлекеттің ақпараттық саясатын қосуға болады. Бұл өз кезегінде ақпараттық соғыс түсінігімен тығыз байланысты. «Жұмсақ күш» – бұл мемлекеттің өз тарапына көптеген жақтастарды тарту стратегияларынан тұрады және оны белгілі бір дәрежеде экономикалық жарнамаға теңестіре аламыз. Жарнамадағы секілді саясаттағы «жұмсақ күш» өз елінің тартымды бейнесі мен имиджін жарнамалап, өзінің жақсы жақтарын, жағымды қасиеттерін және мүмкіндіктерін асыра көрсетуге саналы түрде ұмтылады. Мемлекеттің жұмсақ күш сипатында үстемдік етуі кезінде ел өзінің мәдениетін, саяси идеяларын және бағдарламаларын барынша тартымды етіп көрсетіп, өз құндылықтарының жоғары екеніне тырысып бағып, соған еруге үгіттейді. Егер де аталған стратегиялар мен тактикалардың тиімділігі төмен не жеткіліксіз болса, онда «жұмсақ күш» құралы нысаналы мемлекеттің мәдениетін, құндылықтарын және идеалдарын қаралауға бағытталады.

Әдетте бұл екі стратегия бір мезетте қолданып, бірін-бірі толықтыруы мүмкін. Мұндай технологиялардың негізгі міндетіне – біріншіден, өзінің бәсекелес мемлекетін әлемдік қоғамдастықта ұсқынсыз кейіпте бейнелеп, оның халықаралық тұрақтылыққа қауіп төндіретін субъект ретінде көрсете алуымен, ал екінші жағынан өзінің елін тұрақтылық пен еркіндік мекені ретінде көрсете алуы жатады. Ақпаратты осылайша ұсыну басқа елдермен тиімді саяси, экономикалық, қаржылық, әскери серіктестік орнатуға, өзінің еліне бизнес пен капиталды тарту арқылы тиімді экономикалық және инвестициялық келісім-шарт жасасуға мүмкіндік береді.

Жалпы, уақыт өткен сайын «жұмсақ күштің» ауқымы кеңейіп, ол жаңа аспектілермен толығып келеді. 2019 жылғы «The Soft Power 30» мемлекеттердің «жұмсақ күш» рейтингісіне жүгінетін болсақ, бұл рейтингтік баяндамада елдердің «жұмсақ күш» стратегияларының көптеген қайнаркөздерімен қатар, олардың жаһандық саяси контекстегі ықпалы да көрсетілген. Оған мемлекеттің жаһандану үрдісінің қарқынына үлесі, «жұмсақ күштің» ұлттық үкіметтердің саяси биліктегі рөліне әсер ету деңгейі, мемлекеттік емес субъектілердің елді басқарудағы рөлінің артуына ықпалы, цифрлық (сандық) революция және тіпті климаттың өзгеруіне әсері мен онымен күресуі сияқты аспектілер енген. Сонымен қатар, бұл индексте объективті (мемлекеттің саяси басқару жүйесі, цифрландыру деңгейі, мәдени мұрасы, білім деңгейі, кәсіпкерлікті дамыту көрсеткіштері және т.б.) және субъективті (мемлекеттің басқа елдермен достастық деңгейі, оның асханасының кең танымалдылығы, люксті тауарлары мен брендтері, сыртқы саясаты, халқының тұрмыс деңгейі мен өмір сапасы және т.б.) мәліметтер ескерілген [1]. Мысалы, жалпылама атап өтсек Батыс елдерінің оның ішінде әсіресе АҚШ-тың «жұмсақ күш» стратегиясында «Батыс елдерінің құндылықтарын тарату мен институттарын жаю, басқа мемлекеттер мен қоғамдарға Батыстың түсінігіндей адам құқықтарын қорғау мен құрметтеуге мәжбүрлеу және Батыс үлгісіндей демократияны қабылдау» секілді саясат жүргізу дәстүрлі стратегияға айналған [2]. Сәйкесінше, АҚШ пен НАТО-ның негізгі стратегиясында жалпы адамзаттық құндылықтарды бүкіл әлемге тарату гуманистік мақсаты болғанымен, оны күш қолдану немесе күш қолдану қоқан лоқысын жасау арқылы жүзеге асыруға тырысуы жалпы адамзаттық құндылықтар ұғымына нұқсан келтіруі мүмкін.

**Анықтамалық ақпарат және әдебиеттерге шолу**

Зерттеу барысында «гибридтік соғыстар» феномені халықаралық қатынастар саласындағы салыстырмалы түрде жаңа құбылыс екені анықталды. Бұл терминнің негізін американдық стратег Фрэнк Хоффман 2006 жылы қалады, оның айтуынша «гибридті соғыс» – ол мемлекеттер немесе басқа да қарулы топтар арасындағы жай ғана соғыс емес, оның ауқымы одан да кең. Оған қақтығыстың әртүрлі гибридтік формаларын қолдану кіреді. Онымен қоса «гибридті соғыстар» латентті және жасырын сипатқа ие, ол өте ұзаққа созылуы мүмкін, сондықтан бұл соғыс түрі ешқандай нақты нормативті-құқықтық құжаттармен, доктриналармен, стратегиялрамен, үкіметаралық келісімдермен немесе басқа да құжаттармен реттелмейді. Себебі әлемдік және аймақтық державалардың стратегиялық мүдделеріне қайшы келеді, өйткені олар «гибридті соғыстардың» көмегімен өздерінің мақсат-мүдделерін жүзеге асыруда елеулі табыстарға қол жеткізіп отыр.

**Методология**

Зерттеу жұмысының әдісі- тарихи әдіс,контен анализ әдісі, социологиялық әдістер кешені құрай отыра, гибридті соғыс және оның элементтері талдау көрінеді.

**Жаһандану және «жұмсақ күш»**

Негізінде, қоғамдық сана қашанда елдің ұлттық мәдени-рухани болмысының көрінісі бола отырып, мемлекеттің саяси истиблишменті мен басқару формасында шешуші рөл атқарады. Сондықтан да қоғамдық сананы манипуляциялау кез-келген стратегияның басты нысаны болып табылады. Бұл бағыттағы ең үлкен серіпіліс «тұтынушы қоғам» идеологиясының қалыптасуымен тікелей байланысты, бұл идеология әлемнің барлық дерлік мемлекеттерінде кезең-кезеңмен дәстүрлі құндылықтарды ығыстырып, орнына жаппай тұтыну қағидаттарын қоғам өміріне кіріктіруде. Осылайша, «тұтынушы қоғам» идеологиясы қоғам өмірінің алғашқы тұтыну саласынан бастап оның өнер, мәдени-рухани салаларына дейінгі аралықтағы барлық дерлік салаларына кіріктіріліп келеді. Осы орайда айта кететін жайт, АҚШ және Батыс мемлекеттерінің белсенді түрде насихаттап отырған жаһандану идеологиясы да осындай айлалардың бірі. Жаһандану дегеніміз – бұл дүниежүзілік экономикалық, саяси, мәдени және діни интеграция мен бірігу үдерісі. Ал жаһандану өз кезегінде перифериялық елдердің ұлттық бірегейлігі мен өзіндік ерекшеліктеріне нұқсан келтіреді, оларды жаһандық нарықтан шығуға мәжбүр етеді (өйткені олар бәсекелестікке төтеп бере алмайды), кедей және бай мемлекеттер арасындағы технологиялық және экономикалық алшақтықты арттырады. Осылайша, жаһандану гибридті соғыстың тағы бір құрамдас бөлігі ретінде қызмет етеді. Бұл өркениетті соғыс қағидасына сай оның негізгі логикасы жаулап алған мемлекеттің халқын бытыраңқы етіп, әлсіретіп, орталықсыздандырып, жеңімпаз тараптың еркін орындауға мәжбүрлеу көзделеді. Сондай-ақ ақпараттық құралдарды қолдану арқылы ұлттық құндылықтар мен адамгершілік қағидаттарын бұрмалау, салт-дәстүрлік сананы улау арқылы қоғамды оңай басқаруға болатын тобырға айналдыру мақсаты қойылады.

Дәстүрлі құндылықтар мен әлеуметтік-мәдени көзқарастарды шаюмен ерекшеленетін эгоцентризм идеологиясы «тұтынушы қоғам» идеологиясының үстем факторы ретінде тұлғаның жағымсыз қасиеттері көрінісінің тежеу тетіктерін жою арқылы ақпараттық кеңістікте, тұлға өзінің негативті ойларға құқылы екенін сезіндіре отырып, әлеуметтік желілерде психологиялық зорлық-зомбылық жасау арқылы қоғамда әлеуметтік-психологиялық деформациясын тудыратын агрессивті ортаны қалыптастырады. Әсіресе бұған жастар мен жасөспірімдер сезімтал келеді, өйткені олар компьютерлер мен гаджеттерді қарым-қатынас жасау үшін жиі пайдаланады және олар үшін виртуальды әлемде агрессивті мінез-құлық көрсету заңды әрекет ретінде бағаланады. Киберкеңістікте адамдар өздерінің эмоцияларын, пікірлерін және мінез-құлықтарын еркін

білдіре алады, сондықтан жастардың виртуальды ортаға тәуелділігі артады себебі бұл кеңістікте оларға бір-бірімен танысу, сөйлесу, қарым-қатынас жасау және өздерінің шынайы келбетін ашу оңайырақ. Мұнда жасөспірімдер және кейбір ересектер физикалық әлемде жасай алмайтын нәрселерге құқылымыз деп ойлап, балағат, былапыт және қорлау сөздерін жиі пайдаланады, ал киберкеңістік бұл әрекеттерге мүмкіндік беріп отыр. Ғаламтор жүйесіндегі қорқыту, үркіту, кудалау мен қоқан лоқы көрсетудің жаңа әдістері үнемі жаңаланып, жаңа қосымшалар мен жаңа онлайн форумдарда пайда болады, бұл өз кезегінде аталған қасіретті феноменмен күресуді қиындатып отыр. Соңғы зерттеулерге сүйенсек, жасөспірімдердің жартысына жуығы (49%) Интернетте зорлық-зомбылық әрекеттерін жасаған болса, ал жартысынан көбі (61%) кибербуллингке немесе кибершабуылға ұшыраған [3].

Бүгінде бүкіл әлем ғалымдары бұл мәселенің шығу тегі мен шешу жолдарын іздестіруде, бірақ әзірге нәтижесіз. Өйткені ақпараттық қоғамның қауіпсіздік саласы әліде қалыптасу сатысында. Эмпирикалық зерттеулер мәліметтеріне сүйенсек, алуан түрлі мәдениеттердің аталған факторларға түрлі тежеу функцияларының бар екендігін көрсетіп отыр. Атап өтер болсақ, Ғаламтордағы агрессия мен өшпенділік деңгейі мемлекеттердің ерекшеліктеріне байланысты айтарлықтай ерекшелініп отыр [4]. Мысалы, мәдениеттерінде ұжымшылдық құндылықтары басым, жоғары моральдық қағидаттарға ие, эгалитарлық ұстанымдарының жоғары деңгейімен сипатталатын Шығыс елдерінің тұрғындары, ұжымшылдық мәдениеті төмен Батыс елдерінің тұрғындарымен салыстырғанда агрессияның төмен деңгейін көрсетті. Қытай, поляк және американдық студенттерін зерттеу нәтижесі, мәдениеттегі индивидуализм неғұрлым жоғары болса, соғұрлым олардың бойында тікелей және жанама агрессивті мінез-құлыққа ие екенін көрсетті [5]. Сондай-ақ, қытайлық жасөспірімдер (жәбірленушілер немесе куәгерлер) мұғалімдердің көмегіне жиі жүгіне алатынын білдірді, себебі олар ересектер өздерін қорғайтынына сенімі мол.

Қытай сияқты елдер ақпараттық қоғамды дамытудың кері жақтары мен қауіпті тұстарын түсініп, белсенді сақтық және профилактикалық шараларды қолға алуы ғажап емес. ҚХР-інің төрағасы Си Цзиньпин ақпараттық қауіпсіздік пен киберқауіпсіздіктің маңыздылығын ескере отырып, былай: «Киберқауіпсіздіктің жоқтығы ол – ұлттық қауіпсіздіктің жоқтығымен бара-бар» деп атап көрсетті [6]. Еркеше атап өтетін жайт, Қытайдың және жалпы Азия елдерінің «жұмсақ күш» саясаты Батыстық мемлекеттердің саясатынан біршама ерекшеленеді, өйткені Шығыс елдері үшін қарапайым халық алдында өздерінің оң имиджін қалыптастыру басты мақсат болып табылады және олар өздерінің мәдени, рухани болмысын сақтай отырып, «жұмсақ күш» саясатын қоғамдық және мәдени дипломатия арқылы жүзеге асырады.

Жалпылай алғанда, Қытайдың «жұмсақ күш» саясаты басқа елдердің азаматтарымен қатар, шетелдерде тұратын өздерінің қандастарына да бағытталған, өйткені оларға Қытай үкіметі өз идеологиясын тереңінен түсіндіре отырып, өз мемлекетінің агенттеріне айналуын көздейді. Қытайдың «жұмсақ күш» саясатының мақсаты – өз мәдениетін сыртта дәріптеумен қатар оны ел ішінде сақтап қалу, бірінші жағдайда Қытай «жұмсақ күш» саясатын әлемге өзінің құндылықтарын таңып отырған Батыстың «жұмсақ күшіне» қарсы қойса, екінші жағдайда өзінің территориясында құндылық вакуумының орнын толтыру арқылы мәдениетінің трансформациясын болдырмау мақсаты қойылып отыр. Аталған мақсаттарға жету үшін, Қытай өз құндылықтары мен мәдениетін дәріптеу үшін әлемдік деңгейде фильм түсіретін Голливуд кинокомпанияларына инвестиция құю арқылы өзге елдердің тұрғындарына өзінің құндылықтары мен мәдениетін жарнамаласа, қытайлық тұтынушыларға ұлттық мәдени бірегейлікті үгіттеп насихаттайды. Сәйкесінше, қазіргі таңда Қытай өз азаматтарына (басқа елдердің тұрғандарын қоса алғанда) жоғары сапалы ақпараттық өніммен

қамтамасыз ету мақсатында бұқаралық ақпараттық құралдарын, оның ішінде интернет-БАҚ белсенді түрде дамытуда. Сонымен қатар, білім беру мекемелерін, мәдени туризмді, тіпті дәстүрлі қытай медицинасын «жұмсақ күштің» құралдары ретінде қолданып келеді. Осылайша, қытайлық саясаттанушылар «жұмсақ күш» ұғымын мемлекеттің даму стратегиясын, идеологияның идентификациялық күші мен басым құндылық бағдарларын, әлеуметтік жүйе мен экономикалық модельдің тартымдылығын, ұлттық идеясы мен идеологиясын, ұлттың шығармашылық әлеуеті мен мәдени тартымдылығын қамтитын комбинициялық тұжырым ретінде қабылдайды [7].

Ал Жапония экономикалық модельдің табыстылығына үлкен мән береді. Жапонияның «жұмсақ күш» саясаты экономикалық дамыған мемлекеттермен қарым-қатынасында ұлттық бизнестің мүдделерін ілгерілету арқылы іске асырса, ал нашар дамыған мемлекеттермен қатынасында экономикалық күш пен гуманитарлық көрегендікті көрсету арқылы жүзеге асырады. Алайда, «жұмсақ күштің» негізгі және басты элементі күшті рухани және идеологиялық құрамдас бөлікке негізделуі қажет, өйткені бұл бөліктер бір мезетте шетелдік «жұмсақ күштің» ықпалынан мықты қорғаныс болып, иммунитет қызметін атқарып, ал басқа сыртқы мемлекеттерге күшті ықпал ету құралы қызметін атқаруы мүмкін. Жалпы, бірегейлік саясаты (политика идентичности) – елдің стратегиялық саяси, әлеуметтік, экономикалық тұрақтылықтығын, ақпараттық қауіпсіздігін және «суверенитетті қоғамның тұтастылығын» қамтамасыз етуде мемлекеттің маңызды ресурсы болып табылады [8].

**Ақпараттық соғыс гибридті қауіп-қатердің элементі ретінде**

Ақпараттық соғыс қажетті қоғамдық пікірді қалыптастыруға бағытталған гибридті соғыс пен қауіп-қатердің аса маңызды құрамдас бөлігі екенін атап өту қажет. Оның мақсаты – дұшпанның күшін ыдырату мен жою. Осы мақсатқа жету жолында мемлекет өзінің жақтастарына жаудың халықаралық құқық нормаларын бұзушы қылмыскер екеніне сендіріп, оны талқандау қажеттігін алға тарта отырып, одақтасады. Тиісінше, ақпараттық соғыс екі деңгейде жүргізілуі мүмкін: сыртқы және ішкі деңгей. Сыртқы деңгей дұшпан елдің халықаралық аренадағы беделін түсіру арқылы жүзеге асады. Ал ішкі деңгей қарсылас мемлекетке ақпараттық қару қолдану арқылы оған залал келтірумен қатар қоғамды жасырын (ашық) түрде манипуляциялау арқылы оған психологиялық қысым көрсету стратегияларын қолдану арқылы жүзеге асады. Бұл кезде субъект мемлекет гибридті соғыстың «жұмсақ күш» элементтерін, ықпал ету агенттерін ынталандыру тактикаларын және жаппай азаматтық арандатушылық құралдарын пайдалануға тырысады.

Ақпараттық қару қолдану тактикасы, әдетте, соғыстар мен әскери операциялар кезінді жиі қолданады. Американдық саясаткер Ч.Фриман былай атап өтеді: «соғыс жағдайында жалған электронды хабарламаларды, фейк жаңалықтарды, саяси көшбасшыларға компроматтарды жылдам тарату құралдарын (әлеуметтік желілерді қоса алғанда) қарқынды қолдану дұшпанға орасан зор психологиялық қысым көрсетуге мүмкіндік береді. Осындай әрекеттердің нәтижесінде саяси үйлестіру мен шешім қабылдау үдерісі ретсізденіп, қоғамның жағдайды қабылдауы бұрмаланып, саяси басшылыққа сенімсіздік артады» [9].

Ақпараттық соғыстың келесі мақсаты ұлттың рухани-адамгершілік негіздерін жоюға бағытталған, бұл кезде ұлттық құндылықтарды «жаһандық» құндылықтармен алмастырып, мемлекеттің дәстүрлеріне жат нормалар таңып, қоғамның ақпаратты сыни талдау дағдыларын жоюға бағыттап, объект халықты оңай манипуляциялауға мүмкіндік беретін «желілік қоғам» қалыптастыру. Бүгінде ақпараттық кеңістіктің қоғамдық санаға ықпалы өте жоғары. Бұл ең алдымен, коммуникацияның әмбебеп құралы – Интернет туралы болып отыр. Интернет арқылы біз кез-келген ақпаратты әлемнің кез-келген

нүктесіне оңай әрі жылдам тасымалдау арқылы хабар алмасамыз және оның ең басты артықшылығы ақпаратты нақты адресатқа жеткізе алу мүмкіндігіне ие болуында. Осылайша қажетті ақпаратты нақты тұлғаға жеткізе отырып, оны алуан түрлі әдіспен манипуляциялай алады. Нәтижесінде, белгілі бір идеялар мен мүдделер аясында топтасқан, Интернет пен әлеуметтік желілер көмегімен құрылған сегментті әлемдік қоғам пайда болады. Аталған қоғам мүшелері үшін ұлттық территориалдық аумақ маңыздылығын жоғалтып, жаһандық деңгейдегі іс-әрекеттер алдыңғы орынға шығады. Олар үшін ұлттық мүдде, ұлттық мәдениет, салт-дәстүр және патриотизм ұғымдары жат болып, жаһандық азаматтылыққа ұмтылады.

Зерттеу нәтижелері көрсеткендей, әлеуметтік желілерде жаңғырық камераларының (эхо-камера) ықпалы өте күшті, өйткені олардың жабық қауымдастықтарында (пікірлестер клубы, блогтар, әлеуметтік желілердегі қауымдастықтар, субмәдениеттер және т.б.) қажетті идеялар мен сенімдерді қайта-қайта қайталау арқылы тұлғаның санасына сіңіреді. Тиісінше, мұндай қауымдастықтарға мүше болған адамдар тек өздерінің желілік қоғам мүшелерінің идеялары төңірегі аясында ойланып, сыртқы ақпарат көздері (ұлттық мүдде тұрғысындағы ақпараттарды қоса алғанда) мен басқа пікірлерді еш қабылдамайтын дәрежеге түседі. Оған қоса, аталған блогтарға немесе әлеуметтік желідегі қауымдастықтарға мүше тұлғалардың өзіндік көзқарастары мен сенім-нанымдары, логикалық талқылау мен пікірталас кезінде, толықтай дерлік жойып, оларды жаңғырық камералары аясында оқшаулап, бұғаттайды [10].

Бұл уақытқа дейін басқарушы режимнің оппозиция өкілдерін бір қауымдастыққа біріктіру еш мүмкін болмады, себебі шын мәнінде сізде өзіңізбен пікірлес қанша адам бар екенін білу өте қиын болатын. Онымен қоса өзіңізге жаңа жақтастар тарту күрделі міндеттерден еді, өйткені тиісті ақпарат тарату көптеген қаржылық ресурстарды, құралдарды және таратпа материалдарды талап ететін. Өзге мемлекеттің территориясынан жақтас іздеп, тарту мүлдем мүмкін емес әрекет болатын. Ал қазір ақпараттық құралдардың дамуымен, әлеуметтік желілердің кең таралуымен аталған мақсаттар мен міндеттерге жету өте оңай шаруаға айналды, әлеуметтік желіде өзіңізге лайықты клуб, қауымдастықты тауып, тіркелсеңіз болғаны. Ол қауымдастықтарда қанша жақтас бар екені, олар кімдер екені сияқты алуан түрлі ақпараттарды алу тышқанның бір клигімен ғана қол жеткізуге болады. Жоғарыда атап өтілгендей, әлеуметтік желілер, өзара әрекеттестіктің жаңа формаларын ұсына отырып, қоғамдық сананың приципиалды жаңа түрін қалыптастырады; олар белгілі бір оқиғалар желісін құра отырып, өздеріне қажетті ақпаратты тарата алады және саяси бэкграунды жоқ «пікір көшбасшыларын» аз уақыт ішінде құрап, көсемдері етіп тағайындауға мүмкіндік береді. Сонымен қатар, әлеуметтік желілерде соңғы кездері ақылы троллинг кең етек алып жатыр, мақсаты – әлеуметтік желілерде жағымсыз эмоционалдық жағдайды өрішіте отырып, арандатушылық ақпараттарды орналастыру арқылы қажетті қоғамдық пікірді қалыптастыру. Сондай-ақ ақпараттық соғыстарда астротурфинг және мемдер тарату секілді жаңа әдістер кеңінен қолданылады. Бұлардың барлығы «ақпараттық вирустарды» құру арқылы әлеуметтік желі қолданушыларының саналарын жаппай улауға бағыттылған [11].

Осыған орай, орын алған оқиғаларға және Ғаламтор желісінде жарияланып қойған ақпаратқа кештеуілдеп жауап беру жеткіліксіз екенін түсіну маңызды, өйткені ол ақпараттар жетер жеріне жетті. Мұндай жалған әрі арандатушылық ақпараттардың алдын алу үшін және шынайы жауап қату үшін ресми билік өкілдері елдің ұлттық мүддесінен шығатын превентивті ақпараттық өрісін құру маңызды, себебі жау тараптың ақпараттық вакуумды толтыру қауқарына кедергі келтіре отырып, жағымсыз әсерін азайта алады. Сонымен қатар, қоғамның дәстүрлі БАҚ-тарға деген сенімнің үнемі төмендеп келе жатқанын ескерген жөн [12], және әлеуметтік қоғамдағы белсенді азаматтардың баламалы медиаға яғни әлеуметтік желілер мен мессенджерлерге көбірек жүгінетінін естен

шығармау керек. Сондықтан билік өкілдері ақпараттық белсенділіктің жоғары деңгейін қамтамасыз ете отырып, алуан түрлі жалған әрі арандатушылық ақпарат көздерін тарататын қауымдастықтарды үнемі бақылауында ұстаған жөн. Американдық саясаткер Х.Клинтон жазғандай, «арандатушылық қауымдастықтармен күресудің тиімді жолы оларға тыйым салып, бұғаттау емес, олармен ақпараттық пікірталас алаңында ашық айқасу мен арандатушылық әрекеттерін әшкерелеп, айыптау арқылы жолын кесуге ұмтылу» [13]. Жоғарыда келтірілген әдістер ақпараттық соғыста сәтті жеңіске жетудің азы ғана, қатысушы акторлардың іс-әрекетіне қарай олармен күресудің тиімді стратегиялары мен тактикаларын таңдай білу өте маңызды іс. Осылайша, ақпараттық соғыстың физикалық ұрыспен барабар ұғым екенін түсінуге болады.

**Киберсоғыстар гибридті соғыстың элементі ретінде**

Гибридті соғыс кезінде киберқауіпсіздік ерекше маңызға ие, өйткені қазір технологиялық инфрақұрылым нысандары (объектілері) алуан түрлі бағдарламалық жүйелермен жабдықталған, ал олардың көпшілігі Интернет желісіне байланған. Стратегиялық бағдарламалардың Интернет желісі аясында қызмет етуі ұлттық қауіпсіздікке үлкен қауіптің қайнар көзі болуы мүмкін. Мысалы, маңызды инфрақұрылымдық кәсіпорынға бағытталған хакерлік не компьютерлік шабуыл тек осы объектінің жұмысы мен қызметін толық тоқтатып қана қоймай, сонымен бірге тұтастай ел экономикасына кешенді түрде кері әсер етеді және бұл өз кезегінде елдің және оның азаматтарының қауіпсіздігіне елеулі қауіп төндіреді. Сонымен қатар, кибершабуылдар ақпараттық соғыс аясында көмекші құрал ретінде пайдаланылуы мүмкін, олардың мақсаты құпия деректерді ашу мен жариялау арқылы және фейк (жалған) ақпараттарды жаю арқылы азаматтар арасында дүрбелең туғызу.

Жоғарыда аталған мәселелердің барлығы киберқауіпсіздік мәселесіне жаңалай көзқараспен қарауға итермелейді. Сондай-ақ, халық тіршілігін қамтамасыз ететін жүйелер мен елдің стратегиялық нысандары жайлы сөз қозғалғанда киберқауіпсіздікпен қамтамасыз етудің маңыздылығы арта түседі. Стратегиялық инфрақұрылым нысандарының қызметіне заманауи технологиялардың көмегімен кері әсер етудің жағымсыз салдары өте ауқымды болуы мүмкін, бұл жекелей адам шығындарынан бастап (мысалы, көлік инфрақұрылымын басқарудың автоматтандырылған жүйелері мен электр қуатын басқару жүйелеріне шабуыл нәтижесінде және т.б. техногенді апаттар) елеулі қираулар мен стратегиялық объектілердің (су, электр және атом станцияларының автоматтандырылған жүйелері мен экологиялық қауіпті химиялық өнеркәсіптердің автоматтандырылған жүйелеріне кері әсер ету) істен шығуына дейін алып келуі мүмкін. Онымен қоса, мемлекеттің стратегиялық маңызды экономикалық инфрақұрылымының қызметіне елеулі нұқсан келеді. Сәйкесінше, АКТ-ны қасақана қолдану дәстүрлі қару-жарақ түрлерін қолданумен барабар келетіндей шығынға ұшыратуға қауқарлы, ал кейбір жағдайларда жаппай қырып-жою қаруын қолданғандай зиянға ұшыратуы әбден мүмкін [14].

Технологиялық процесстерді басқарудың автоматтандырылған жүйелеріне кибершабулыдардың негізгі мақсаты – технологиялық процесстерді критикалық (апаттық) деңгейге жеткізу арқылы критикалық күй айналымы мәндерінің операциялық шегінен шығарып, елеулі зақымдар мен апаттарға ұшырату. Мұндай шабуылдың мысалына, 2010 жылы Иранның ядролық нысандарын келтіруге болады, жау тарап бұл нысандарда Stuxnet компьютерлік вирусын пайдаланған. Stuxnet вирусы турбогенераторлардың айналу жиіліктерін рұқсат етілген эксплуатациялық межеден күрт арттыру немесе түсіру арқылы істен шығаруға бағытталған. «Адами факторға» байланысты Stuxnet вирусы Бушер АЭС-ның бірқатар компьютерлерін залалға ұшыратты, алайда бұл бүкіл станцияның жұмысына

әсер етіп, апатқа ұшыратпады, себебі турбина бөлімінің компьютерлеріне вирус жұқпаған [15].

Американдық барлау агенттіктері ұлттық инфрақұрылым саласына кибершабуылдардың ауқымды статистикасын жинақтаған, бұл статистикаларға сүйенсек, елдің тұтас экономикасы мен инфрақұрылымының қызметіне елеулі нұқсан келтіру мақсатында оның энергетика секторы кибершабуылдардың басты нысаны болып табылатынын көрсетеді. Жыл сайын электр станцияларының ақпараттық желілеріне 18 мыңнан 20 мыңға дейін шабуыл әрекеттері тіркеледі, бұл өз кезегінде барлық ұлттық инфрақұрылым нысандарына кибершабуылдардың орта есеппен 35%-ын құрайды [16]. Яғни, миллиондаған қарапайым адамдардың өмірін және қажеттіліктерін қамтамасыз ететін нысандар (инфрақұрылымдық маңызды нысандар) тікелей кибершабуылдар мен инсайдерлік шабуылдарға осал болып келеді.

Стратегиялық маңызды инфрақұрылымды қорғау барлық мемлекеттердің ортақ мәселесіне айналып отыр, бұл киберқаруды ядролық қарумен тең дәрежедегі тежеу элементі ретінде қарастырып, халықаралық деңгейде аталған нысандарға кибершабуылдардың жол берілмейтіндігін және оның үлкен қылмыс екенін мойындау мәселесін күн тәртібіне шығарды. Алайда бүгінгі күні ақпараттық кеңістікте мемлекетаралық қатынастарды реттейтін халықаралық-құқықтық нормалар жоқ, ал қолданыстағы халықаралық заңнамалар ақпараттық және киберқауіпсіздік мәселелеріне қолданыла алмайды. «Бұл жағдай негізінен аталған саланың аса саясиландырылғандығына байланысты болып отыр, өйткені киберәлеуеті өте жоғары алып державалар (АҚШ, Ресей, Қытай) мен орта державалардың арасындағы мүдделер (әскери, экономикалық, әлеуметтік, дипломатиялық) қақтығысы мен қайшылықты ұстанымдары, ортақ шешімге жетуге кедергі келтіруде», деп батыс сарапшылары санайды .

Осы уақытқа дейін принципиалды тармақтар бойынша еш келісім келу мүмкін болмай отыр, мысалы киберкеңістіктегі егемендік тұжырымдамасын қалай жүзеге асыру керек, өзін-өзі қорғау мен тиісті қарсы шараларды қалай іске асыру қажет секілді тармақтар өте даулы. Дәстүрлі ұғымда жоғарыда аталғандарды белгілі бір аумақтық территориямен байланыстыра алсақ, алайда ақпараттық кеңістікте субъектілердің қандай да бір территориялық аумақсыз қызмет етуі мен материалдық нысандармен еш байланыссыз әрекет жасауы мәселенің күрделілік деңгейін арттырады. Сондықтан, ағылшын ғалымдары Tsagourias N. мен Buchan R. пайымдауынша мемлекеттің суверенитеті мен юрисдикциясы тек сол елдің территориясымен шектелмейді, өйткені олар мемлекеттер киберкеңістік саласында экстерриториалдық юрисдикцияға ие деп есептейді [17].

Дәл осы тәсіл 2018 жылы АҚШ-та қабылданған «Бұлт актісі (Cloud Act)» деп аталатын заңда жүзеге асырылған болатын, онда АҚШ өзінің юрисдикциясын шет елдерде орналасқан серверлерге де жүретінін белгіледі. Бұл заңның қабылдануы Microsoft корпорациясы мен АҚШ-тың Әділет министрлігі арасындағы даумен байланысты, АҚШ-тың құқық қорғау органдары Microsoft корпорациясынан американдық юрисдикцияға жатса да жатпаса да әлемнің кез-келген жеріндегі пайдаланушылардың электрондық пошта деректеріне еркін қолжетімділігін талап еткеннен кейін аталған заңды қабылдау үдерісі басталды. Осы кезде Microsoft корпорациясы деректердің біраз бөлігі Дублинде орналасқан серверлерде сақталатынын, яғни оларға Ирландияның суверенитеті жүретінін алға тартып, пайдаланушылардың электрондық пошта деректеріне еркін рұқсат беруден бас тартқан еді. АҚШ-тың Жоғарғы соты да Microsoft корпорациясын қолдады, себебі 1986 жылғы «электрондық байланыстардың құпиялылығы туралы» заңға сай АҚШ-тан тыс территориялардағы деректерге қол жеткізуге тиым салынған. Осы сот шешімі қабылданғаннан кейін АҚШ үкіметі өзінің құқық қорғау органдарына шетелдегі интернет пайдаланушылардың деректеріне қол жеткізуді қамтамасыз ететін «Бұлт актісі (Cloud

Act)» заңын бірден қабылдады. Бұл заң аясында АҚШ үкіметі әлемдегі кез-келген электрондық коммуникациялардың мазмұнын ашуға, оларды провайдерлерде сақтауға және резервті көшірмелерін жасауға, клиенттің кез-келген жазбасы мен оның жеке мәліметтерін беруге, абоненттің провайдерлері туралы ақпаратты беруге компанияларды мәжбүрледі. Американдық ірі компаниялардың трансұлттық сипатын ескерсек, онда АҚШ-тың кибер суверенитеті мен юрисдикциясы бүкіл әлемге дерлік таралуда деп айтуға негіз бар. Оған қоса, бұл заң аясында жергілікті заңнамалардың ақпаратты бермеу күші жүрмейді, АҚШ сұраған деректер міндетті түрде берілуі тиіс.

Екінші жағынан Ресей үкіметі мен заң органдарының ұстанымы белгілі бір дәрежеде киберқауіпсіздік қамтамасыз ету тұрғысынан аумақтық факторды негізге алады. Яғни, белгілі бір территорияда ақпараттық инфрақұрылымның физикалық орналасуы оның қалыпты жұмыс істеуін толық бақылауға алуға, демек, киберкеңістікті де қадағалауға мүмкіндік бере отырып, ал бұл өз кезегінде мемлекеттің кибершабуылдардан, киберқылмыстардан, кибертыңшылықтардан және киберқақтығыстардан қорғануға мүмкіншілік береді [18]. Осы орайда, айта кететін жайт, бүгінде әлемде 13 DNS серверлері (негізгі серверлер) қызмет етеді, оның 10-ы АҚШ-тың территориясында, 2-уі Еуропалық Одақта, ал 1-уі Жапонияның аумағында орналасқан. Соңғы жылдары әртүрлі елдердің өз серверлерін жасауға ұмтылғанымен, негізгі ақпарат ағындары АҚШ-та орналасқан негізгі серверлер арқылы өтеді. Осылайша, антагонисттік мемлекеттер болып отырған Ресей мен АҚШ-тың киберқауіпсіздік саласындағы ұстанымдары да бір-біріне қарама-қайшы күйінде. Ресей ақпараттық инфрақұрылым аумақтық орналасуын қолдаса, ал АҚШ негізгі ақпараттық ағындарының өзінің серверлері арқылы өткендіктен, керісінше өзінің кибер суверенитетін бүкіл әлемге таратуға ұмтылуда.

Одан бөлек, әлемде маңызды инфрақұрылымдарды құрайтын нысандар туралы жалпы ортақ түсінік жоқ, ал бұл өз кезегінде оларды қорғаудың түрлі әдіс-тәсілдерін қарастыру барысында, мүдделердің қайшылығына алып келеді. Сонымен, АҚШ үшін маңызды инфрақұрылым – ол «мемлекет үшін өте маңызды болып табылатын физикалық немесе виртуалдық жүйелер мен құралдар жиынтығы. Егер ондағы нысандардың аз бөлігі істен шығып, жарамсыз болса, онда бұл мемлекеттің ұлттық қауіпсіздігіне, денсаулық сақтау жүйесіне, экономикасына, қорғаныс саласына елеулі зардаптар келтіруі мүмкін». Осы анықтамаға сай, АҚШ-тың маңызды инфрақұрылымы 16 негізгі секторды қамтиды: химия, энергетика және байланыс, қауіпті өндірістер, ядролық реакторлар, гидроқұрылыстар, сумен жабдықтау жүйелері, әскери-өнеркәсіптік кешендер, төтенше жағдайлар қызметі, тамақ секторы және ауылшаруашылығы, медицина және денсаулық сақтау жүйелері, ақпараттық технологиялар, көлік жүйелері, қалдықтарды басқару жүйелері, қаржы және коммерциялық секторлар және мемлекеттік органдардың штатты режимде қызмет етуі.

Еуропалық Одақ (ЕО) үшін маңызды инфрақұрылым – бұл мүше мемлекеттердің аумақтарында орналасқан, қоғамның өмірлік функцияларын қамтамасыз ету үшін, денсаулық, қорғаныс, қауіпсіздік салаларының дұрыс қызмет етуі үшін, адамдардың экономикалық және әлеуметтік әл-ауқатын көтеру үшін қажетті активтер жүйесі немесе оның бөлігі. Оған қоса, аталған сала нысандарының бірінің істен шығуы немесе қирауы одаққа мүше елдердің өз функцияларын орындауға айтарлықтай әсер етсе, бұл да маңызды инфрақұрылымның көрсеткіші. Осыған орай, ЕО-ның маңызды инфрақұрылымы тоғыз секторды құрайды: энергетика, транспорт, сумен жабдықтау, денсаулық сақтау, АКТ, қаржы және сақтандыру, мемлекеттік және әкімшілік қызметтер, азық-түлік және ауылшаруашылығы, медиа және мәдени құндылықтар [19].

**Қорытынды**

Қорыта айтсақ, геостратегиялық, геоэкономикалық тұрғыда қарастырылған кибершабуылдар елдің бүкіл экономикасына әсер етіп, құлдыратуға қауқарлы, саяси көзқарастарды өзгертуге әлеуетті, мемлекетаралық және мемлекетішілік қақтығыстарды қоздырту мүмкіндігіне ие, саяси акторлардың әскери тиімділігін төмендете алады, жоғары технологиялық әлеуетке ие елдердің деңгейін төмен технологиялық мемлекеттермен теңестіруге қауқарлы болғандықтан кибер қауіпсіздік мәселесінің өзектілігі аса зор.

«Түрлі-түсті революциялар» гибридті қауіп-қатердің элементі ретінде қарастырар болсақ.

Жоғарыда атап өтілгендей, гибридті соғыс аясында жүргізілетін «жұмсақ күш» саясатының мақсаты дәстүрлі құндылықтарды жойып, орнына жат псевдоқұндылықтарды алып келу арқылы орнын алмастыру және қалыптасқан саяси жүйеге, билік органдарына және саяси көшбасшыларға теріс көзқарас қалыптастыруға күш салу. Ал ақпараттық соғыстың түпкі мақсаты – дұшпан мемлекет халқының санасын манипуляциялау арқылы өз азаматтарының қолымен оның мемлекеттілігінің іргесін шайқалту мен қирату. Осы мақсатқа жету үшін жергілікті тұрғындардан «ықпал ету агенттері» мен «пікір жетекшілері» таңдалып, пайдаланылады, олардың міндеттері наразылық акцияларын, билікке қарсы арандатушылық әрекеттерін және саяси биліктің беделін түсіретін бұқаралық шараларын ұйымдастыру болып келеді. Бұл әрекеттердің барлығы түптеп келгенде «түрлі-түсті революцияларға» ұласатын азаматтық бағынбау әрекеттеріне алып келетін қоғамдық наразылық атмосферасын құруға бағытталады.

Жалпы «түрлі-түсті революциялардың» құрылымын шартты түрде 3 сатылы (ярустық) пирамида түрінде көрсетуге болады. Ең жоғары сатығы наразылықтың демеушілерін орналастыра аламыз. Бұлар азаматтарды үйретіп, бағыт-бағдар беріп, қаржыландыратын және наразы топтарды ақпараттық қолдаумен айналысатын тұлғалар топтары. Олар өздерін ешқашан әшкере етпейді, олар тек қана арадағы делдалдар арқылы әрекет етеді. Осылайша, аталған «демеушілер» бүкіл әлемдік қауымдастық алдында өздерінің лайықты келбетін сақтай алады. Орта сатыны төңкерісті тікелей ұйымдастырушылар құрайды. Бұл категорияға пиар және насихат саласындағы мамандар (журналистер, кәсіби психологтар) кіреді, олар халық бұқарасының революциялық көңіл-күйін, саяси билікке қарсы жағымсыз көзқарасты қалыптастыруға ат салысады. Ұйымдастырушылардың бұл категориясына шешендер мен харизмамен ерекшеленетін жас саясатшылар да кіруі мүмкін. Үшінші сатыны ең көп бұқара – қала алаңдар мен көшелеріндегі наразылық акцияларына шыққан адамның көп екендігін көрсетуге қажет қарапайым адамдар мен халық. Олардың бір бөлігі идеологиялық көзқарасы бойынша шынайы көтерілісшілер болса, ал басқа бөлігі ақша үшін митингке шыққан адамдар болуы мүмкін. «Түрлі-түсті революциялардың» мақсаты мемлекеттік төңкеріс болғандықтан, демеуші топтың мүддесі шектеулі уақыт ішінде осы мақсатқа жету үшін барын салады, сондықтан олар гибридті соғыс жүргізу әдістері мен технологияларын барынша қолданады [20].

Осы орайда «түрлі-түсті революциялардың» американдық идеологы Джин Шарп оның 3 кезеңін атап көрсетеді: 1. наразылық акциялары, митингілер, марштар, пикеттер арқылы азаматтарды биліктің легитимділігіне күмән туғызып, үкіметке қарсы қозғалысты қалыптастыру; 2. заң қорғау құрылымдарының беделін түсіру, ереуілдер, қоғамдық бағынбау, тәртіпсіздіктер мен саботаж; 3. Билікті күш қолданбай құлату [21]. Бұл орайда атап өтер жайт, «оппозиция көшбасшыларының» негізгі рөлі нақты әрі іс жүзінде жүзеге асырылатын іс-қимыл бағдарламасын тұжырымдап ұсыну емес, наразы адамдарды (өмір сүру деңгейінің экономикалық және әлеуметтік жағдайына қанағаттанбайтындарды, өздерінің шығармашылық әлеуеттерін жүзеге асыра алмағандарды, жеке өмірлеріне қанағаттанбайтындарды) оппозиция қатарына қосу бағдарламаларын жариялау болып табылады. Хоффман атап өткендей, бұқаралық қозғалыстар аталған наразылық деңгейін

бір арнаға бағыттаумен, белсенді әрекеттер арқылы жеке тұлғалардың өздерінде ықпалды күш бар екенін сездіру. Азаматтардың өзіне деген жоғалған сенімі «маңызды іске үлес қосудамын» деген сеніммен алмастырылады. Жаппай қозғалыстарға қатысу қатысушы тұлғаларға үміт пен өмірлеріне мән береді деген пікір бар [22].

Тиісінше, «түрлі-түсті революцияларды» азаматтардың наразылық деңгейі жоғары, саяси тұрақсыз және экономикалық-әлеуметік жағдайы төмен мемлекеттерде оңай жүзеге асыруға болады. Ал саяси жүйесі тұрақты мемлекеттерде төңкерісті гибридті соғыстың келесі элементтерін: ақпараттық соғыс, кибершабуылдар, шекарасы маңындағы шиеленісті тұрақ түрде өршіту, ел ішіндегі лаңкестер мен сепаратистерді қолдану арқылы жүзеге асыруға болады. Мемлекеттің аталған тактикаларға қарсы іс-қимылдардың маңызды тетіктері әлеуметтік-экономикалық жағдайды үнемі бақылап, азаматтардың қанағаттану/қанағаттанбау деңгейіне тұрақты мониторинг жасау қажет, бұны заманауи АКТ-ны қолдану арқылы қол жеткізуге болады. Сондай ақ, пайда болған наразылықты бәсеңдету үшін жедел әрекет ету қажет, өйткені «бұқаралық қозғалыс алып күшке айналып, мемлекеттің маңызды стратегиялық нысандарының штаттық режимде жұмыс жасауына кері әсер етеді». Сондықтан, ұлттық қауіпсіздік саласында қызмет ететін органдар, гибридті соғыс пен қауіп-қатерлердің алдын алу үшін кешенді әлеуметтік-экономикалық, саяси-әскери шаралармен қамданғаны жөн.

Қорытындылай келе, «түрлі-түсті революциялар» белгілі бір саяси жүйелерге ықпал ету бағдарламасы болып табылады, ол белгілі әдістер мен тактикаларға негізделеді, ал оларға қарсы күресу барысында кешенді стратегиялық іс әрекеттерді жоспарлы түрде жүзеге асыру өте маңызды.

**Әдебиеттер**


1. The Soft Power 30 (2019) // https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf, дата обращения 20.04.2022.
2. Брычков А.С. и др. (2019) Гибридные войны XXI столетия: происхождение, сущность и место в цивилизационном процессе: Монография. Смоленск.
3. Calpbinici P., Arslan F.T. (2019) Virtual Behaviors Affecting Adolescent Mental Health: The Usage of Internet and Mobile Phone and Cyberbullying // Journal of Child and Adolescent Psychiatric Nursing, vol. 32, no 3, pp. 139–148. DOI: 10.1111/jcap.12244
4. Song M., Zhu Zh., Liu Sh., Fan H., Zhu T., Zhang L. (2019) Effects of Aggressive Traits on Cyberbullying: Mediated Moderation or Moderated Mediation? // Computers in Human Behavior, vol. 97, pp. 167– 178. DOI: 10.1016/j.chb.2019.03.015
5. Yuchang J., Junyi L., Junxiu A., Jing W., Mingcheng H. (2019) The Differential Victimization Associated with Depression and Anxiety in Cross-cultural Perspective: A Meta-analysis // Trauma, Violence & Abuse, vol. 20, no 4, pp. 560–573. DOI: 10.1177/1524838017726426
6. Разумов Е.А. (2017) Киберсуверенитет как аспект системы национальной безопасности КНР // Россия и Китай: история и перспективы сотрудничества. Материалы VII международной научно-практической конференции. С. 707–710 // https://elibrary.ru/ item.asp?id=29191372, дата обращения 20.04.2022.
7. Сургуладзе В.Ш. (2019) Политика идентичности в реалиях обеспечения национальной безопасности: Стратегия, теория, практика. М.: С.Т.К.
8. Политика «мягкой силы» Китая в Азии (аналитический доклад РИСИ) (2019) // Проблемы национальной стратегии. № 3. С. 11–67 // https://riss.ru/ bookstore/journal/2019-g/3-54/, дата обращения 20.04.2022.
9. Фриман Ч. (2018) Технологии, государственное управление и неограниченная война // Россия в глобальной политике. № 1 // http://www.globalaffairs.

ru/number/Tekhnologii-gosudarstvennoe-upravlenie-i-neogranichennaya-voina-19349, дата обращения 20.04.2022.
10. Виловатых А.В. (2018) Использование информационно-коммуникационных технологий в военно-политических целях: социально-психологический аспект // Проблемы национальной стратегии. № 2. С. 197–211 // https://riss.ru/images/pdf/journal/2018/ 2/09.pdf, дата обращения 22.04.2022
11. Breden J. (2013) Intell Tool Would Track Social Media like a Virus // GCN Magazine, February 12, 2013 // https://gcn.com/articles/2013/02/12/intell-tool-track-social-media-like-a-virus. aspx, дата обращения 05.05.2022.
12. Николайчук И.А., Янгляева М.М., Якова Т.С. (2018) Крылья хаоса: Масс медиа, мировая политика и безопасность государства. М.: Икар.
13. Clinton H. (2011) Internet Rights and Wrongs: Choices & Challenges in a Networked World // U.S. Department of State, February 15, 2011 // https://2009-2017. state.gov/secretary/20092013clinton/rm/2011/02/156619.htm, дата обращения 20.05.2022.
14. Вильданов М., Башкиров Н. (1) (2019) Международно-правовые аспекты защиты инфраструктуры государств от киберугроз // Зарубежное военное обозрение. № 7. С. 3–10 // http://factmil. com/publ/soderzhanie/informacionnye_ vojny/mezhdunarodno_pravovye_aspekty_zashhity_infrastruktury_gosudarstv_ ot_kiberugroz_2019/107-1-0-1659, дата обращения 10.05.2022.
15. Калашников А.О., Сакрутина Е.А. (2018) Прогнозирование рискового потенциала объектов критической инфраструктуры атомных электростанций // Управление развитием крупномасштабных систем. М.: Институт проблем управления им. В.А. Трапезникова РАН. С. 245–247 // https://elibrary.ru/ item.asp?id=36620660, дата обращения 10.05.2022.
16. Вильданов М., Башкиров Н. (2) (2019) Международно-правовые аспекты защиты инфраструктуры государств от киберугроз // Зарубежное военное обозрение. № 8. С. 21–26 // http://factmil.com/publ/soderzhanie/informacionnye_ vojny/mezhdunarodno_pravovye_aspekty_zashhity_infrastruktury_gosudarstv_ ot_kiberugroz_2019/107-1-0-1659, дата обращения 21.04.2022.
17. Tsagourias N., Buchan R. (eds.) (2015) Research Handbook on International Law and Cyberspace, Sheffield: Edward Elgar Publishing.
18. Joubert V. (2010) Getting the Essence of Cyberspace: A Theoretical Framework to Face Cyber // Conference on Cyber Conflict Proceedings, Tallinn // https://ccdcoe.org/uploads/2018/10/Jou- bert-Getting-the-Essence-of-Cyberspace. pdf, дата обращения 10.05.2022.
19. Разумов Е.А. (2017) Киберсуверенитет как аспект системы национальной безопасности КНР // Россия и Китай: история и перспективы сотрудничества. Материалы VII международной научно-практической конференции. С. 707–710 // https://elibrary.ru/ item.asp?id=29191372, дата обращения 20.04.2022.
20. Freyer Nathan. 2009. The Defense Identity Crisis: It's a Hybrid World. W http://strategicstudiesinstitute.army.mil/ubs/parameters/articles/09autumn/freier.pdf/.
21. Брычков А.С. и др. (2019) Гибридные войны XXI столетия: происхождение, сущность и место в цивилизационном процессе: Монография. Смоленск
22. Катунин Ю. А. «Цветные революции»: методология и методы организации // Ученые записки Крымского федерального университета имени В. И. Вернадского. Социология. Педагогика. Психология. 2014. №1. URL: https://cyberleninka.ru/article/n/tsvetnye-revolyutsii-metodologiya-i-metody-organizatsii (дата обращения: 22.04.2022).

***Резюме***

*Известно, что XXI век характеризуется эпохой глобализации. В этом контексте все человечество строит тесные отношения друг с другом. Все человечество рассчитывало на этот век как на новую эру глобального сотрудничества. Но этот век полон политических противоречий и обретает характер во всех формах безопасности. Современный этап международных отношений характеризуется уменьшением важности стандартных тактик ведения войны, таких как борьба с противником на поле боя, создание стратегий и тактик для его преодоления и победа. Сейчас военная мощь государства превращается из основного фактора его мощностей в один из таких факторов, как информационные, экономические, политические, культурные, демографические, финансовые возможности этой страны. Таким образом, возможности государств решать проблемы только военной силой уменьшились, и им пришлось использовать новые дополнительные ресурсы на фронтах войны, то есть различные гибридные стратегии. Прежде чем начать говорить об использовании тактики и технологий «мягкой силы» в современном мире, стоит кратко остановиться на значении понятий и терминов, имеющих отношение к данному термину. Таким образом, в научном сообществе понятие» гибридная война «включает в себя дипломатическое и экономическое давление на противника, организацию» цветных революций", кибербезопасность, хакерские атаки и шпионаж с целью оказания давления на потенциального противника наряду с вооруженными (осуществляемыми с использованием вооруженных (военных, частных военных компаний, повстанческих ополченцев) конфликтов между смертельными государствами как создание благоприятного информационного пространства, так и применение принципов мирного воздействия. Действительно, мирный период гибридной войны, который может быть использован государством, включает использование стратегии «мягкой силы». Большая часть теории игр движется к позициям развитых государств. Изменчивое существование теории игр, происходящих в мире, требует знания элементов гибридных войн государств с появлением гибридных угроз, возрастающих признаков больших и малых войн, а также мягкой силы. Каждое государство определяет свои основные элементы, прежде чем бороться с гибридными угрозами. Государства мира по-своему борются с гибридной угрозой. В будущем Штаты могут даже не заметить гибридную угрозу, поскольку она может произойти в самых разных ситуациях. В этой связи возникла необходимость изучения основных элементов гибридной угрозы в рамках центральноазиатских государств, которые не сильно проникли на историческую сцену.*

***Abstract***

*It is known that the XXI century is characterized by the era of globalization. In this context, all of humanity is building close relationships with each other. All mankind counted on this century as a new era of global cooperation. But this century is full of political contradictions and acquires a character in all forms of security. The modern stage of international relations is characterized by a decrease in the importance of standard tactics of warfare, such as fighting the enemy on the battlefield, creating strategies and tactics to overcome it and victory. Now the military power of the state is turning from the main factor of its capacity into one of such factors as information, economic, political, cultural, demographic, financial capabilities of this country. Thus, the ability of states to solve problems only by military force decreased, and they had to use new additional resources on the war fronts, that is, various hybrid strategies. Before we start talking about the use of tactics and technologies of "soft power" in the modern world, it is worth briefly focusing on the meaning of concepts and terms related to this term. Thus, in the scientific community, the concept of "hybrid war" includes diplomatic and economic pressure on the enemy, the organization of "color revolutions", cybersecurity, hacker attacks and espionage in*

*order to put pressure on a potential enemy, along with armed (carried out using armed (military, private military companies, rebel militias) conflicts between deadly states both create a favorable information space and apply the principles of peaceful influence. Indeed, the peaceful period of hybrid warfare, which can be used by the state, includes the use of a "soft power" strategy. Most of the game theory is moving towards the positions of developed countries. The changeable existence of the theory of games taking place in the world requires knowledge of the elements of hybrid wars of states with the emergence of hybrid threats, increasing signs of large and small wars, as well as soft power. Each state defines its main elements before dealing with hybrid threats. The states of the world are fighting the hybrid threat in their own way. In the future, the States may not even notice the hybrid threat, since it can occur in a variety of situations. In this regard, it became necessary to study the main elements of the hybrid threat within the framework of the Central Asian states, which did not penetrate much into the historical scene.*

UDC 327.8

**[1]Aidarbek Amirbek, [2]Taha Barut**
[1] Associate Professor, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkestan, Kazakhstan. e-mail: aidarbek.amirbek@ayu.edu.kz
[2] 2Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkestan, Kazakhstan. e-mail: Tahababaev@tutanota.com

## ONE BELT, ONE ROAD: ANALYSIS OF A GLOBAL INITIATIVE

***Abstract***

*The "One Belt, One Road"(BRI) initiative is a large-scale economic and infrastructure initiative put forward by China in the early 21st century, aiming to connect Asia, Europe and Africa via land and sea routes. This initiative is presented as a modern reflection of the historical Silk Road. The basic structure of the BRI is based on a broad network covering many countries and regions. Different land and sea corridors aim to increase trade and connectivity between regions. In addition to economic benefits, participating countries are also directly supported with infrastructure and development projects. On the economic dimension, BRI offers large-scale investments and trade opportunities. China has made generous investments in financing projects, increasing its global economic influence. However, it has been observed that these investments also bring with them concerns about debt. In the context of political and strategic relations, the BRI is seen as a tool to increase China's global influence. However, there is also local resistance and concerns in some countries. The dynamics between China's strategic objectives and the expectations of participating countries are complex. In terms of technology and infrastructure, projects under the BRI include modern technologies and sustainable practices. The Digital Silk Road is an important component that promotes digital connectivity between regions. Socio-cultural dimensions show that the BRI is not just an economic initiative. Intercultural interaction, educational exchanges and tourism are other important benefits brought by the initiative. Sustainability and environmental issues have raised concerns about the impacts of infrastructure projects. Despite this, green development and sustainability principles will shape the future of the BRI. The initiative has faced several challenges, including funding challenges, debt trap concerns, and management challenges. However, there is much speculation regarding the future of the BRI, its role in the global political economy, and its potential expansions. In conclusion, "One Belt, One Road"stands out as a complex initiative with both positive and negative aspects. Future developments will determine how the global impact of this large-scale project will be shaped.*

## МАЗМҰНЫ / СОДЕРЖАНИЕ / CONTENT

### *ТЕХНИКАЛЫҚ ҒЫЛЫМДАР/ ТЕХНИЧЕСКИЕ НАУКИ/ TECHNICAL SCIENCES*



### *ГУМАНИТАРЛЫҚ ҒЫЛЫМДАР / ГУМАНИТАРНЫЕ НАУКИ / HUMANITARIAN SCIENCES*

## *ЗАҢ ҒЫЛЫМДАРЫ / ЮРИДИЧЕСКИЕ НАУКИ / JURIDICAL SCIENCE*

## *ПЕДАГОГИКАЛЫҚ ҒЫЛЫМДАР / ПЕДАГОГИЧЕСКИЕ НАУКИ / PEDAGOGICAL SCIENCES*