УДК 327.8

АҚШ-ҚЫТАЙ ҚАТЫНАСТАРЫНДАҒЫ КИБЕРҚАУІПСІЗДІК МӘСЕЛЕСІ

Алимжанова Толғанай Қайратқызы
a.tolganai@inbox.ru
Л.Н. Гумилев атындағы ЕҰУ Халықаралық қатынастар факультетінің
Халықаралық қатынастар кафедрасының 3 курс студенті,
Нұр-Султан, Қазақстан
Ғылыми жетекшісі – Джумадилова Г.М.

Киберқауіпсіздік тұжырымдамасы жақында пайда болды, ол көпқырлы және көптеген компоненттермен сипатталады. Зерттелген АҚШ пен Қытайдың елдерінің кибер кеңістігін басқарудағы принциптері әр түрлі. АҚШ киберқауіпсіздікті халыққа ақпарат қол жетімділігіне кепілдік беру тұрғысынан түсіндіреді. Азаматтық бостандықты және жеке өмірге қол сұғылмаушылықты қорғау АҚШ-тың киберкеңістік саясатына қатысты іс жүзінде жарияланған барлық заңнамаларындағы негізгі мақсат болып табылуда.Қытайда киберқауіпсіздік саласындағы саясатты қалыптастыру процесінде елдің басшылығы Интернеттің рөлінің артуына, елдердің әлемдік киберкеңістіктегі өзара тәуелділігіне, сондай-ақ болуы мүмкін қауіп-қатерлерге назар аударады, сондықтан ішкі интернетті бақылауды қажет деп санайды және оны жүзеге асырады.

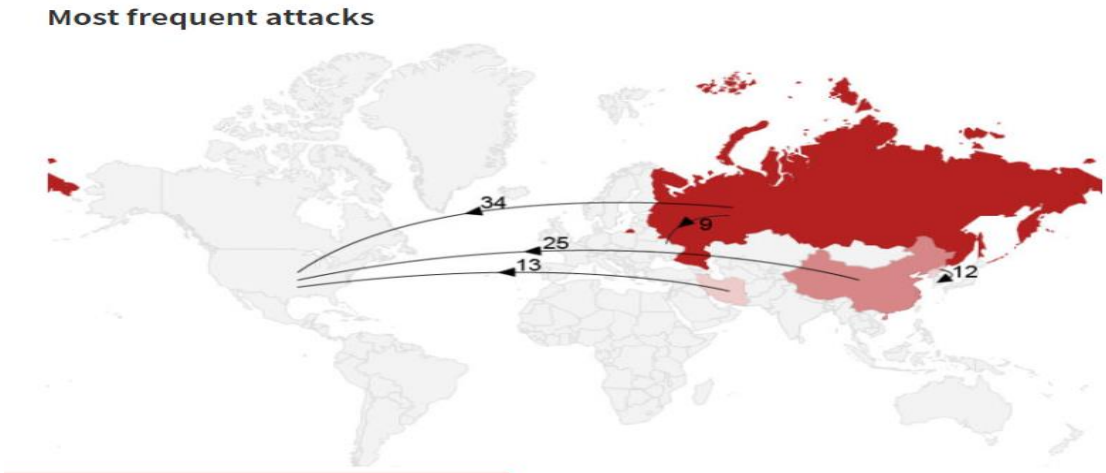
Терминологиядағы айырмашылық өз кезегінде екі елдің проблемаға деген әртүрлі көзқарастарын көрсетеді. АҚШ-та «киберқауіпсіздік» термині ең алдымен интернет архитектурасының қауіпсіздігін қамтамасыз етуге қатысты жиі қолданылатын болса, Қытайда (Ресейдегі сияқты) қажет емес ақпаратты таратуға шектеулерді білдіретін «ақпараттық қауіпсіздік» термині қолданылады[1]. Мақсаттар мен тәсілдердің айырмашылығы АҚШ пен Қытай арасындағы диалогты қиындатады.

Жалпы киберқауіпсіздік мәселесіне алаңдау 2011 жылғы қыркүйек айындағы трактілерден кейін қарқынды өсе бастады. Дәл осы кезде халықаралық деңгейде алғашқылардың бірі – АҚШ болды. АҚШ Президенті Барак Обама 2011 жылдың маусым айында Халықаралық киберкеңістік стратегиясына қол қойды. Жаңа жылғы стратегия - бұл АҚШ-тағы мемлекеттік ақпараттық қауіпсіздік жүйесінің қалыптасуының жиырма жылдық тарихының нәтижесі.

Тұтастай алғанда, Обама әкімшілігінің негізгі стратегиялық құжаттарында халықаралық қатынастардың қалыптасып келе жатқан жүйесі полицентрлік екендігі бірнеше

рет айтылды. Көптеген «ұлттық стратегиялардан» айырмашылығы – құжаттың «Киберкеңістіктің халықаралық стратегиясы» деп аталатындығы. Әкімшілік мұны жасай отырып, АҚШ-тың ақпараттық қауіпсіздік саясатындағы басты өзгерісті - халықаралық ынтымақтастыққа баса назар аударуды көздеген болатын[2]. Дональд Трамп әкімшілігі де осы бағытты жалғастырды, бұған қоса, киберкеңістікте АҚШ-қа қарсы кибершабуыл жасайтын адамдарға немесе топтарға қарсы халықаралық санкциялар енгізу мүмкіндігінқарастыра бастады.

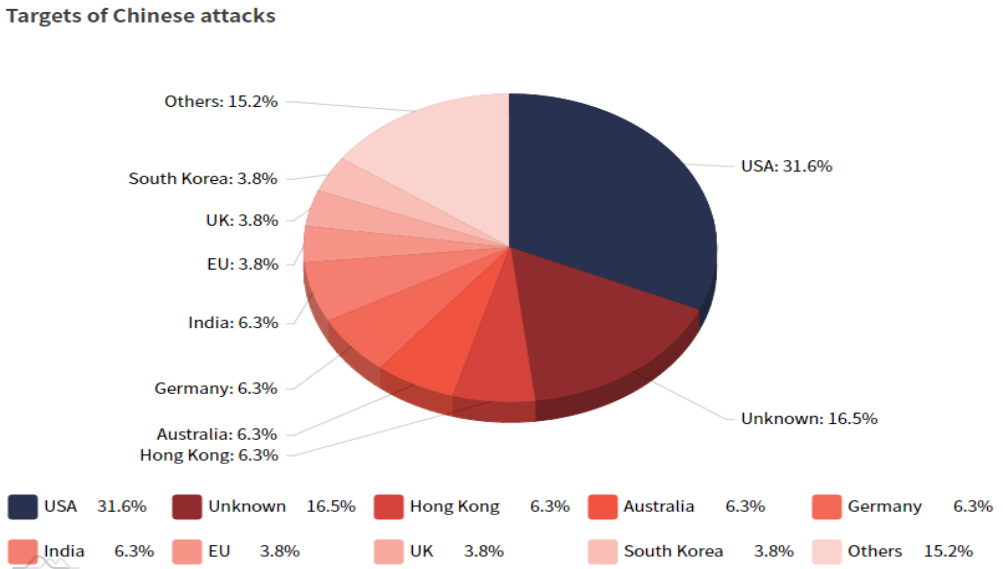
Сурет-1. Ең жиі шабуылдар жасалатын мемлекеттер [3;1].



Source	Target	Attacks
Russia	USA	34
China	USA	25
Iran	USA	13
North Korea	South Korea	12
Russia	Ukraine	9

Кейбір елдер кибер соғыс оқиғаларының қайнар көзіне айналуда, ал кейбіреулері ең жиі нысандарына айналады. 2009 жылдан 2019 жылға дейін Ресей, Қытай және Иран АҚШ-қа жалпы 72 рет шабуыл жасады, бұл әлемдегі шабуылдардың шамамен 15% құрайды. Бұл жерде АҚШ-қа қарсы басты қарсыластардың бір бағытта әрекет етуін байқауға болады, оны Иран, Ресей мен Қытай жазылмаған «серіктестігі» деп атауға да болады, себебі осы елдер арасындағы бір-біріне кибершабуылдар саны жоқтың қасы.

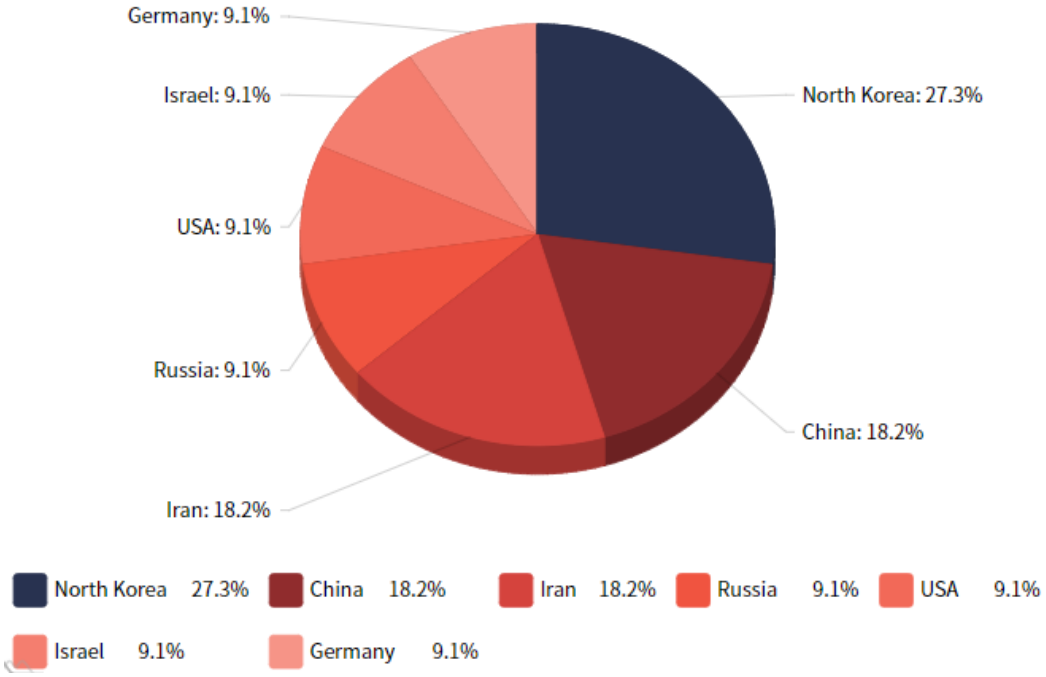
Сурет-2. Қытай шабуылдарының нысандары[3;2].



Қытай шабуылдарының 32% -ы АҚШ-қа бағытталды, бұл АҚШ-ты қытай хакерлерінің ең үлкен нысаны етеді. Әскери тұрғыдан Қытай өзін АҚШ-қа қарағанда әлсіз держава деп санауға болады, бұл оны асимметриялық реакция стратегиясын жасауға мәжбүр етеді. Мұндай стратегияның элементі зымырандық қорғаныс спутниктік басқару жүйелеріне және американдық кибер кеңістіктің басқа элементтеріне араласуды қамтуы мүмкін. Сонымен қатар, Қытай ішкі мәселелерді шешу үшін киберкеңістіктегі конфронтацияны белсенді пайдаланады.АҚШ экономикасы Қытай экономикасына қарағанда кибер кеңістікке әлдеқайда тәуелді.

Соңғы 20 жылда БҰҰ осы саладағы мәселелерді талқылауға арналған негізгі халықаралық алаң болды. 2018 жылдың күзінде АҚШ халықаралық қауіпсіздік мәселесінде мемлекеттердің киберкеңістіктегі жауапкершілікті мінез-құлқын ілгерілету туралы өзінің шешімін ұсына отырып, 2018 жылдың күзінде тағы да осы саладағы халықаралық ынтымақтастық мәселесін күн тәртібіне қойды. 2018 жылдың қыркүйегінде Трамп әкімшілігі дайындаған АҚШ-тың «Ұлттық кибер стратегиясы» жарияланды. Құжатта көрсетілген негізгі қауіп - АҚШ-тағы бостандық пен демократияға қауіп, ал олардың басты көздері - Ресей, Қытай, Иран, Солтүстік Корея деп көрсетіліп, олар халықаралық терроризм тәуекел көздеріне жатқызылды.

Сурет-3.АҚШ-тың кибершабуылдарының нысандары [3;3].



Көріп тұрғанымыздай, ең көп кибершабуыл АҚШ-тан үш мемлекетке: Солтүстік Корея (27,3%), Қытай және сәйкесінше Иранға (18,2%) қарсы бағытталған. Бұл АҚШ-тың ұлттық киберқауіпсіздік стратегиясыментұспа-тұс келеді, осы саладағы басты қауіптер ретінде АҚШ дәл осы елдерді жатқызатынын аңғаруға болады және сәйкесінше саясат жүргізетінін болжауға болады.

АҚШ-та басқа мемлекеттердің шабуылы ретінде жамылып манипуляция жасауға мүмкіндіктері бар (ЦРУ мысалында). Америка Құрама Штаттарында киберсоғыстың бұл түрі конгресстің мақұлдауын қажет етеді.

Қазіргі уақытта Қытайдың ақпараттық қауіпсіздікке деген көзқарасы американдықтардың Интернеттің ашықтығы туралы түсінігімен қайшы келеді. Қытайды Қытайдың Батыс елдеріне технологиялық тәуелділігінің ұзақ мерзімді келешегі алаңдатады. Олардың тәуелсіздікке жету стратегиясы өзінің технологиялық инновацияларын енгізуге және американдық компанияларға бәсекелестік туғызуға негізделген. Оған сәйкес қолданыстағы

жоспарларға сәйкес, 2020 жылдың соңына қарай ҒЗТКЖ-ға(ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстар) шығындар ЖІӨ-нің 2,5% -ын құрауы керек, ал 2049 жылға қарай Қытай инновацияларды жүзеге асыруда жетекші орынға ие болуды жоспарлап отыр. Бұл үшін оның қолында айтарлықтай адами ресурстар бар: жыл сайын алты миллионнан астам түлектің 60-70% ғылыми-техникалық мамандар мен инженерлер құрайды)[4].

Қытайда барлық биліктің бір қолда шоғырлануы ақпараттық кеңістіктегі саяси бағыт үшін идеологиялық фактордың маңыздылығын арттырып көптеген мүмкіндік береді.Сөз бостандығы мен жеке өмірге құқықты шектеу үшін билікке карт-бланш береді. Халық тоталитарлық езгі, қуғындау, ақпарат қауіпсіздігінен айырылады. Соңында бұл жаппай наразылық өсуіне әкелуі мүмкін.Және иберкеңістікті «жұмсақ күш» саясатын тарату үшін пайдалану, яғни Қытай имиджін көтеруші шаралар жүргізу, жағымды пікір қалыптастыру, мәдени танымдық материалдарды желілерде тарату ж.т.б. Ал кибершпионаж үшін арнайы жауапты халық-босатушы армияның (НОАК) N61398 бөлімі (2006 ж. қ. Шанхайда базасы бар) бөлімі бар.

АҚШ-Қытай киберконфликтерінің себептері әртүрлі:

- Мемлекетік ақпараттық структураны бұзу, үлттық қауіпсіздкке әсер етер құпия ақпаратқа қол жеткізу, барлау қызметін жүргізу;
- Зияткерлік меншік ақпаратын, технологияларды ұрлау;
- Жеке ықпалды азаматтардың ақпаратын ұрлап, сату (сонымен қатар, осы тәсілмен «шпиондар» анықталады);
- Жаһандық киберқауіпсіздік саласындағы лидерлік үшін ақпараттық-технологиялық жарыс ж.т.б.

Киберқауіпсіздікке назардың өсуі келесі факторлармен негізделді:

- Басқа елдерден артта қалмау, жаһандық киберқауіпсіздік саласындағы лидерлік: бұл халықаралық нормаларды құрудағы айрықша дауысқа қол жеткізуге көмектеседі.
- Әлсіз инфраструктураны қорғай алмау қаупі
- Терроризм қаупі
- Киберкеңістікке шетелдік күштер енуі, қоғам санасына манипуляцилар жүргізу қаупі
- Ұлттық қауіпсіздікке нұқсан келтірер құпия ақпартты, мемлекеттік аппаратты қорғау
- Зияткерлік меншікті қорғау ж.т.б.

Қытай мен АҚШ-та киберқылмыстың артуына байланысты ақпараттық қауіпсіздік саласында ортақ байланыс нүктелері де бар. Қытай да, АҚШ та басты инфрақұрылымға террористік кибершабуыл жасау мүмкіндігіне қатты алаңдайды.

Соңғы жылдары қытайлық жеке және институционалдық инвесторлар Израильдің шағын инновациялық компанияларын сатып алуда бұрын-соңды болмаған белсенділік танытты. Оларды негізінен израильдік технологиялар интернет, киберқауіпсіздік, медициналық жабдық, баламалы энергия көздері, ауылшаруашылық технологиялары сияқты салалар қызықтырады. Оның үстіне қытай инвесторларын осы нарықтағы қатысуын азайтуға мәжбүр еткен Қытай мен АҚШ арасындағы қарама-қайшылықтың күшеюі аясында, 2016 жылы ҚХР-дан Израильдің жоғары технологияларына салынған инвестициялардың бұрын-соңды болмаған өсуі байқалды. Егер 2015 жылы Израиль компанияларына қытайлық инвестиция көлемі миллиард доллардан аз болса, онда 2016 жылы ол 16,5 миллиард долларға жетіп, таңғаларлық көрсеткішке жетті[5]. Израиль АҚШ жағынан басты серіктестердің бірі боп табылады, АҚШ-тың Израильдің Қытаймен технологиялар саласындағы жақындасуына ресми түрде қарсы позициясына қарамастан, ол үдеріс тек өсе түседі деп болжау жасауға болады, бұл қытайлықтардың батыстан технологиялық артта қалуы мен тәуелділігін азайтуға көмектестеді.

Осылайша, бүгінде Қытай Израильді өзінің инновациялық экономикасын дамытудағы перспективалы серіктестердің бірі ретінде қарастырады деп сеніммен айтуға болады. Көптеген жылдар бойыбір мемлекетке, яғни АҚШ-қа ғана сүйенген Израиль үшін жаңа инвестициялық

әлеуетке ие серіктестің пайда болуы қаражат көздерін әртараптандыруды және тағы бір үлкен нарықтың пайда болуын білдіреді. Сонымен қатар, егер АҚШ-пен ынтымақтастықта Израильді кіші серіктес ретінде қабылдайтын болса, Қытай үшін Израиль технологияларының маңызы өте зор, сондықтан Израиль өзін қалыптасып келе жатқан серіктестіктің толық тең құқылы қатысушысы ретінде сезіне алады.

АҚШ пен Канада киберқауіпсіздік саласында, әсіресе «Бес көз» альянсы арқылы ынтымақтастық орнатады. Одақ Екінші дүниежүзілік соғыстан басталады және құрамына АҚШ, Ұлыбритания, Канада, Австралия және Жаңа Зеландия кіреді. АҚШ кибер-барлаудың айтарлықтай дамыған қабілетіне ие, ал «Бес көз» серіктестігі қосымша ақпарат алуға мүмкіндік береді. Канададағы киберқауіпсіздік индустриясы өте жақсы дамыған және ол АҚШ, Ұлыбритания және Австралияның басшылық қағидаттары мен басымдықтарына ұқсайды. Бұл ынтымақтастықты тиімдірек етеді, дегенмен, күрделі технологияның шектеулілігіне байланысты АҚШ пен «Бес көз» серіктестерінің арасында мүмкіндік алшақтығы бар. АҚШ әлемдегі ең бай серіктес болып табылады және Канаданың техникалық жағынан күрделі жағдайына байланысты Канада НАТО-ның аппаратура, бағдарламалық жасақтамасын және персоналын пайдаланады. Сонымен қатар, Бес Көз және Канада елдерімен ынтымақтастық АҚШ-қа ғаламдық бақылау кеңістігін кеңейтудің және Солтүстік Американың киберқауіпсіздігін күшейтудің маңызды құралы болып табылады.

Лиссабонда өткен НАТО саммитінде АҚШ киберқауіпсіздікті бірінші кезектегі мәселеге айналдырды және Солтүстік Атлантикалық шарттың 5-і бабы киберкеңістіктегі әрекеттерге қатысты да таралады деп мәлімденген[6]. Альянстың командалық-басқару жүйелеріне немесе энергетикалық желілерге ауқымды шабуыл 5-бапқа сәйкес ұжымдық қорғаныс реакциясына әкелуі мүмкіндігін атап өту де маңызды.

Сонымен, АҚШ пен Қытай арасындағы киберкеңістіктегі негізгі қақтығыстар мен дауларды талдаудан кейін, елдер арасында басқа салалардағы саяси келіспеушіліктердің жалғасына айналған текетірес бар екендігі аңғарылады. Қытайлық тыңшылық (негізінен коммерциялық), американдық тыңшылық әрекеттеріне біраз уақыт болды. Екі елде де ақпараттық технологиялардың даму деңгейі АҚШ пен Қытай арасында өзара қысымды арттырып, саяси, іскерлік және экономикалық мүдделерге қатысты қатынастар шеңберінде киберқауіптерді туғызады. Бұл Қытай мен АҚШ арасындағы киберқауіпсіздік туралы диалогты одан әрі өзекті және маңызды етеді. АҚШ пен Қытай үшін бірлескен шешімдер қабылдаудың қиыншылығына қарамастан, екі ел әлі байланыс орнатады және әртүрлі деңгейдегі кездесулер өткізеді, бірлескен келісімдерге қол қояды, киберкеңістік сияқты ортақ бағыттың маңыздылығын және терроризмді қоса алғанда, оларға қарсыбірлескен қызметті үйлестіруді және ынтымақтастықтыарттыруды қажет ететін жалпы қатерлердің бар екенін түсінеді.

Киберкеңістіктегі ортақ стратегияны қабылдауды талқылай отырып, екі мемлекет те Интернеттегі жалпыға бірдей қабылданған мінез-құлық нормалары болмаса, халықаралық ынтымақтастық мүмкін емес екендігіне ортақтасады.Бірақ АҚШ және ҚХР-дың Интернет пен ақпарат бостандығына деген көзқарастарына келсек, ол бойынша позициясы тұрақты және өзгереді немесе жеңілдіктерге барады деп айту екіталай. Әлемдік киберкеңістіктің негізгі ойыншылары ретінде ҚХР да, Америка Құрама Штаттары да киберкеңістіктегі бірыңғай нормаларды әзірлеуде және орнатуда бірлескен ынтымақтастықтың дивидендтеріне үміттене алады. Кибер кеңістігінде қалыптасқан өзара сенімсіздік жалпы екіжақты қатынастарға кері әсерін тигізетіндіктен, нормаларды белгілеудегі серіктестік олардың арасындағы шиеленісті төмендетуі мүмкін. Сонымен қатар, АҚШ пен ҚХР-дың осы мәселені шешудегі ынтымақтастығы қауіпсіз ғаламдық кеңістікті қамтамасыз етуге бағытталған көпжақты халықаралық күш-жігерді ілгерілетудегі іргелі қадам бола алады.

Пайдаланылған әдебиеттер тізімі

1.Антипов К. Киберконфликт в китайско-американских отношениях и поиски диалога / К. Антипов // Проблемы Дальнего Востока. 2013. № 6. С. 39 — 54.

2.Булавин А. О подходах США и Китая к обеспечению кибербезопасности / А. Булавин // Общество: политика, экономика и право. 2014. № 1. С. 27.
3.Robinson, J. Cyberwarfare statistics: A decade of geopolitical attacks / Privacy affairs : [сайт]. — URL: https://www.privacyaffairs.com/geopolitical-attacks/ (қаралу күні: 21.11.2020).
4.Лаумулин, М. Т. Основные противоречия между США и КНР на современном этапе / М. Т. Лаумулин. // ISCA : [сайт]. — URL: (қаралу күні: 16.10.2020).
5.Zhu J., Cohen T. China's tech money heads for Israel as U.S. welcome wanes / Reuters : [сайт]. — URL: https://www.reuters.com/article/us-china-investment-israel-idUSKBN187080 (қаралу күні: 16.11.2020).
6.Ждан, О. Е. Стратегия США и НАТО в сфере кибербезопасности / О. Е. Ждан. — Текст : электронный // ISCA : [сайт]. — URL: https://isca.kz/ru/analytics-ru/1794 (қаралу күні: 16.11.2020).