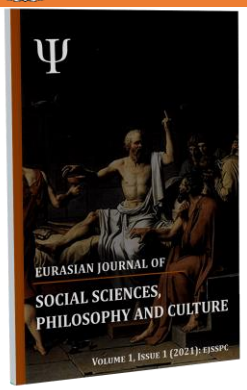
EURASIAN JOURNAL OF SOCIAL SCIENCES, PHILOSOPHY AND CULTURE
Innovative Academy Research Support Center
UIF = 8.2 | SJIF = 6.051 www.in-academy.uz



ХОРИЖИЙ ДАВЛАТЛАРДА КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШНИНГ СТРАТЕГИК МАҚСАДЛАРИ, ВАЗИФАЛАРИНИНГ СИЁСИЙ ТАХЛИЛИ

Батиров Фарход Авазович
Ўзбекистон Республикаси Жамоат хавфсизлиги университети Ўқув-услубий бошқармаси, ўқув жараёнини режалаштириш бўлими бошлиғи
E-mail: Farxod-batirov@mail.ru, Тел: 97 750 91 49
https://doi.org/10.5281/zenodo.7604849

ARTICLE INFO

Received: 22th January 2023
Accepted: 30th January 2023
Online: 31th January 2023

KEY WORDS

Кибер-макон, кибертаҳдид, киберхавфсизлик, миллий хавфсизлиги, киберхужум, кибермудофаа, ахборот хавфсизлиги.

ABSTRACT

Мазкур мақолада хорижий давлатларда киберхавфсизликни таъминлашнинг стратегик мақсадлари, вазифалари ва асосий ҳақида сўз юритилади. Шунингдек, бугунги глобаллашув ва ғоялар таҳдиди авж олган бир пайтда киберхавфсизликни таъминлашнинг муҳим жиҳатлари таҳлил этилган. Хусусан, қуролли можароларда ахборот технологияларидан фойдаланишнинг халқаро сиёсий оқибатларини таҳлил қилиш мамлакатимизда ҳарбий қурилишнинг устувор йўналишларини аниқлаш бўйича таклифлар ва хулосалар берилган.

Кириш. Дунё шиддат билан ўзгариб, барқарорлик ва халқларнинг мустаҳкам ривожланишига рахна соладиган турли янги таҳдид ва хавфлар пайдо бўлаётган бугунги кунда маънавият ва маърифатга, ахлоқий тарбия, ёшларнинг билим олиш, камолга етишга интилишига эътибор қаратиш ҳар қачонгидан ҳам муҳимдир [1 Б-27].

Кибер-макон, биринчи навбатда, компьютерлар ва компьютер хотираси орқали дунёда ишлатиладиган очиқ майдон тушунчасини англатади. Маълумотларга кўра, кибермакон атамаси илк бор 1984-йилда Уилям Гибсоннинг “Burning Chrome” романида қўлланган [2]. Француз файласуфи Пер Левининг фикрича, киберфазо силлиқ, юқори аниқликдаги, интерактив ва виртуал реал вақт маконидир. Бу макон ахборотни қабул қилиш, узатиш, моделлаштириш ва ёзиб олиш имконини беради [3].

Замонавий даврнинг асосий таҳдидларидан бири бу киберҳужумлардир. Кибермакондаги хавф янги ҳодиса эмас. Замонавий кибермакон миллий хавфсизлик нуқтаи назаридан мудофаа тизимини яратишни тақозо этмоқда. Чунки компьютер ва интернет технологиялари кўплаб муҳим соҳаларни бошқариш ва улардан фойдаланишда кенг қўлланилади ва бу ҳар қандай вақтда киберҳужумлар натижасида ушбу тизимларнинг ишдан чиқишига олиб келиши мумкин. Хакерлар (hacker инглизча сўздан олинган бўлиб, hack синдириш, синдириш маъноларини билдиради. Дастлаб хакер деганда дастурлаш даражаси юқори бўлган шахс тушунилган эди) муҳим давлат тизимлари, шу билан бирга, улар ҳам ҳарбий тизимларни фалаж қилишга қодир [4]. Давлатлар баъзан улар билан курашишга ожиз. Шу боисдан ҳам бугунги кунда “Дунёда глобаллашув давом этаётган ва ахборот маконида ўзаро кураш кучайган шароитда

мудофаа тизимида ахборотнинг психологик хавфсизлигини таъминлаш механизми соҳасида бир қатор илмий тадқиқот ишлари амалга оширилмоқда. Бу борада, айниқса, ахборот-коммуникация маконида давлат суверенитети, мустақиллиги, ҳудудий яхлитлигига қарши қаратилган ҳамда аҳолининг тинч ҳаётига таҳдид солувчи мафкуравий ва психологик ҳаракатларнинг илмий-назарий ва амалий ечимини топиш алоҳида аҳамият касб этмоқда"[5 Б-5].

Мавзуга оид адабиётларнинг таҳлили (Literature review). Корнел университетида таҳсил олган ва отаси Миллий хавфсизлик бюросида ишлаган 23 ёшли фуқаро Роберт Моррис ҳукуматга қарашли ARPANET (бугунги интернет "ахборот тармоғи")да ўз-ўзидан кўпаядиган вирусни жойлаштирди. Вирус 6000 та компьютер маълумотлар тармоғига тез тарқалиб, ҳукумат ва университет компьютерларига киришни тўсиб қўйди. 1988 йилда Моррис томонидан интернетга киритилган вирус кўплаб компьютерларни яроқсиз ҳолга келтирди. Моррис Корнелл университетидан ҳайдалди, уч йил ҳибсда сақланди ва 10 минг доллар жаримага тортилди [6].

1990-йилда узоқ давом этган терговдан сўнг АҚШ махсус хизматлари 14 та шаҳарда йирик "хакерлик операцияси"ни бошлади. Операцияда компьютер, кредит карта ва телефон фирибгарлиги учун кўплаб одамлар қўлга олинди. Операция хакерлик гуруҳларига катта зарба берди. Айни пайтда хакерларнинг амнистия эвазига бир-бирини сотиб юбориши улар ўртасида бўлинишга олиб келди. Бу операция тарихга Сандевил операцияси номи билан кирди [7].

Қайд этиш жоизки, замонавий даврда ҳар дақиқада кибермаконда 500 миллион ҳужум ташкил этилмоқда ва бундай ҳужумларнинг 95 фоизи фойдали деб топилган. Дунёнинг юрак уришини ураётган кибер-макон, интернет сайтлари, ижтимоий тармоқлардаги саҳифалар можаролар майдонига, аксарият масалалар ҳал қилинадиган самолётга айланиб бормоқда. Бир қатор давлатлар ўзларининг ахборот устунлигини таъминлаш мақсадида ўзларининг маълумотларини ҳимоя қилиш мақсадида рақиб тармоқларига зарар етказиш учун маълум воситалардан фойдаланадилар ва бу баъзан жуда жиддий оқибатларга олиб келади. Бинобарин, кибермакондан келаётган ҳар қандай таҳдиддан ҳимояланиш учун ўзини-ўзи ҳимоя қилиш тизими доимо тезкор жавоб бериш босқичида бўлиши, мудофаа учун эса кибермакон, интернет ва ижтимоий тармоқлар яратган имкониятлардан самарали ва пухта ўйланган ҳолда фойдаланиш зарур. Бу ҳақида Раҳмон Қўчқор қуйидагича фикр юритади: "Ўзига "ахборот дунёси", "ахборотлашган жамият" деб ном қўйиб олган бугунги жумла жаҳонда у ёки бу воқеа-ҳодиса ҳақида (у тарихда юз берганми ёки куни кеча содир бўлдими – фарқи йўқ) оммавий ахборот воситалари "топиб" тарқатаётган маълумот, "тезкор хабар" қанча кўпайса, ўша воқеа-ҳодисага доир асл ҳақиқат шунча мавҳумлашиб бормоқда" [8 Б-24].

Хорижий мамлакатларда Э.Сэрра, Т.Паренти ва бошқа олимлар ушбу муаммонинг турли жиҳатларини ўз соҳалари йўналишларидан келиб чиқиб тадқиқ қилганлар. Жисмоний шахслар, корхоналар ва ҳукуматлар учун киберхавфсизлик хавфининг интернетига тегишли илғор қурилмаларнинг кўпайиши билан ортиб бормоқда. Компьютер хавфсизлиги, киберхавфсизлик ёки ахборот технологиялари хавфсизлиги компьютер тизимлари ва тармоқларини махфий маълумотларнинг чиқиб кетишидан,

аппарат, дастурий таъминот ёки электрон маълумотларнинг ўғирланиши ёки шикастланишидан, шунингдек улар тақдим этаётган хизматлардаги носозликлар ва узилишлардан ҳимоя қилиш сифатида яққол намоён бўлади [9].

Мустақил давлатлар ҳамдўстлиги мамлакатларидан И.Л.Сафронова, Е.А. Соловьева ва бошқа шу каби олимлар томонидан муаммонинг ҳуқуқий, сиёсий ва ижтимоий-маданий жиҳатлари батафсил ўрганилган. Мазкур тадқиқотлардан маълум бўладики, сунъий интеллект киберхавфсизликда истиқболли ва у асосан таҳдидларни аниқлаш тизимлари билан боғлиқ. Автоматлаштириш нафақат ҳар қандай бузилишлар аниқланишини таъминлайди, балки заиф бўлимларни ҳам ҳимоя қилиши мумкин. Чуқур ўрганиш имкониятлари энди тармоқ таҳдидларини аниқлаш учун журналлар, транзакциялар (маълумотлар трафиги) ва маълумотларни кузатиш учун фойдаланилмоқда. Машинанинг ўз-ўзини ўрганиш имкониятлари барча мумкин бўлган изларни топиш ва аномалияларни аниқлашни ўз ичига олади. У тузилмани таниб олишни “ўрганиш” ва потенциал ҳужум уринишлари ҳақида огоҳлантириш қобилиятига эга, шунингдек, киберхавфсизлик таҳдидларини олдини олиш учун такрорий хатти-ҳаракатларни мослаштириши ва яшириши мумкин. Бундай инновацион технологиялар кундан-кунга такомиллаштирилмоқда [10].

Мамлакатимизда М.Х.Рустамбаев, С.Ю.Аҳроров, И.Ю.Иноятов, З.Ш.Алимардонов, Р.Самаров ва бошқалар ахборот ва жамоат хавфсизлигини таъминлашнинг турли жиҳатларини ўрганишга алоҳида эътибор қаратганлар [11].

Тадқиқот методологияси (Research Methodology). Ҳарбий соҳадаги ўзгаришлар, хусусан, сунъий интеллектнинг қурол тизимлари ва ҳарбий технологияларга интеграциялашуви, автоном қурол тизимларининг ривожланиши кибермаконни ҳарбий ҳаракатлар учун муҳим соҳага айлантирди. XXI асрнинг етакчи рақиблари бўлмиш АҚШ ва Хитой ўртасидаги стратегик муносабатлар бунинг ёрқин далилидир.

Қўшма Штатлар аллақачон киберқуролларни ядровий бўлмаган стратегик ҳужумнинг асосий элементи сифатида кўради ва бу мамлакатнинг 2018 йилдаги ядровий позицияси шарҳига киритилгани бежиз эмас. Кибероперациялар 2010 йилги АҚШ ҳаво кучлари доктринасида ҳам мустаҳкамланган [12].

Хитой, ўз навбатида, Қўшма Штатларга эргашди ва кибер қуролларни ўз эҳтиёжларига мослаштирди. 1990-йилларнинг охирида Хитой Интеграциялашган тармоқ электрон уруши концепциясини ишлаб чиқди. Бу концепция устунликка эришиш мақсадида душманнинг ахборот инфратузилмасини киберҳужумлар ва радиоэлектрон урушлар орқали йўқ қилишни назарда тутади [13].

Хитойлик экспертлар АҚШнинг ахборот технологияларидан кенг фойдаланишини ҳам кучли, ҳам заиф томонлари деб билади. Хитойнинг сиёсий ва ҳарбий раҳбариятининг ахборот технологиялари ва ахборот қарама-қаршилигига қанчалик аҳамият бераётганини Хитой Марказий ҳарбий комиссияси 2004-йилда эълон қилган “Келажак уруши – ахборот технологиялари қўлланиладиган маҳаллий уруш” деган директивада кўриш мумкин. 2005 йилда “келажак уруши” атамаси “келажакнинг компьютерлашган уруши” атамаси билан алмаштирилди [14].

Америка Қўшма Штатлари ва Хитойнинг бу соҳада кучайиб бораётган имкониятлари Хитойнинг келажакдаги ядросиз ҳужуми учун асосий восита бўлади. Шунинг учун у Хитойни кибермакондаги асосий рақобатчиси деб билади. Албатта, яна бир рақобатчи – Россия ҳисобланади. Хитой ўзининг кенг кўламли ва муваффақиятли кибеpразведка операциялари билан машҳур: 2009-2011 йилларда бешинчи авлод жангчилари ҳақидаги маълумотларнинг ўғирланиши, 2015 йилда АҚШнинг 21 миллион федерал ходими ҳақидаги маълумотларнинг тортиб олиниши, Марказий разведка бошқармаси тизимига хакерлик ҳужуми ва бошқалар. Хитойнинг бу соҳадаги кучи давлат инвестициялари ва машиналарни ўрганиш технологиясини ривожлантириш учун ишлатилиши мумкин бўлган улкан маълумотлар базаларидир. Шундай қилиб, дунёнинг учта йирик ядровий давлати АҚШ, Хитой ва Россия ядровий қуролларни етказиб бериш учун янги платформалар яратиш мақсадида учувчисиз ва автоном қурол тизимлари устида ишламоқда. Ушбу платформалар рақобатчиларнинг асосий мақсадига айланмоқда. Жумладан, Украина можароси кўтарган муҳим савол унинг АҚШ киберстратегиясининг келажагига таъсири, хусусан, Пентагоннинг 2018 йилда бошланган “олдинга мудофаа” ёндашуви билан чамбарчас боғлиқ. Гарчи ушбу концепция атрофидаги мунозараларнинг аксарияти АҚШ киберстратегиясининг ролига қаратилган. Гарчи ушбу концепция атрофидаги мунозараларнинг аксарияти ҳужумкор кибероперацияларнинг роли ҳақида бўлса-да, иттифоқчилар ва ҳамкорлар билан ҳамкорлик келажакка йўналтирилган мудофаанинг муҳим, аммо камроқ тан олинган элементидир. Стратегияга кўра, Мудофаа вазирлиги “ушбу иттифоқчилар ва ҳамкорлар салоҳиятини кучайтириш ва Мудофаа вазирлигининг ўз ҳамкорларининг ноёб имкониятлари, ресурслари, имкониятлари ва истиқболларидан фойдаланиш қобилиятини оширишга” ҳаракат қилади [15].

Таҳлил ва натижалар (Analysis and results). Уруш пайтида ҳужумкор кибероперацияларнинг самарадорлиги ҳақида фикр билдирган кўплаб Европалик сиёсатчилар ва кузатувчилар Украинага қарши кенг кўламли кибероперациялар ҳали амалга оширилмаганлигидан ҳайратда қолишди. Бу, айниқса, ҳайратланарли, чунки Россиянинг стратегик тафаккури анъанавий ҳарбий кучни, шунингдек, қўмондонлик ва бошқарув тизимларини таъминлайдиган ёки тўлдирадиган муҳим инфратузилмани нишонга олишда кибероперацияларнинг ролини концептуал тарзда белгилайди. Дарҳақиқат, АҚШ ва Европа расмийлари кибер уруш Россиянинг дастлабки кампаниясининг муҳим хусусияти эмаслигини айтишди. Масалан, Накасоннинг айтишича, Россия сўнгги ҳафталарда Украинага қарши “бир неча” киберҳужумлар уюштирган бўлса-да, хакерлик даражаси урушгача “биз кутгандек” бўлмаган. Кейинчалик у НСА Россиянинг Украинага уч ёки тўртта киберҳужумни кузатганини ва келажакда тўлов ҳужумлари эҳтимоли ҳақида огоҳлантирганини айтди. Европа Иттифоқи расмийлари ҳам “киберҳужумлар сезиларли даражада ошганини кўрмаганликларини” айтишди.

Бир қатор потенциал тахминлар Россия кампаниясининг дастлабки босқичларида кенг кўламли кибер урушнинг йўқлигини тушунтириши мумкин. Жанг майдонида ҳал қилувчи таъсирга эришиш учун кибермакондан фойдаланиш мантиғида эмпирик ёрдам йўқ. Ўтган тажриба шуни кўрсатадики, киберфаолиятлар ишончни сусайтириш

ва ахборот устунлигига эришишда фойдали бўлиши мумкин, аммо улар жанг майдонига унчалик таъсир қилмайди. Хусусан, битта фараз кўпроқ тадқиқотга муҳтож: муваффақиятли кибермудофаа ва Украинада барқарорликнинг роли.

Оммавий ахборот воситаларида АҚШ бир неча ойдан бери Украинага кибермудофаа ишларида ёрдам бераётгани ҳақида кўплаб хабарлар тарқалган. АҚШ Киберқўмондонлиги ўтган декабр ойида Украина тармоқ операторларини қўллаб-қувватлашини эълон қилганидан сўнг, Nyu-York Tayms 7 март куни "кибер-миссия гуруҳлари" деб номланувчи АҚШ Киберқўмондонлиги кучлари Россиянинг рақамли технологияларига аралашишга тайёрлигини хабар қилди. Хужумлар ва алоқалар, лекин уларнинг муваффақият даражасини ўлчаш қийин.

Financial Timesнинг қайд этишича, "Украина ва АҚШ расмийлари" кибермиссия гуруҳлари ишини "мудофаа" сифатида таърифлашда эҳтиёткор бўлишди. Қўшма Штатлар томонидан ҳимоя чораларига қўшимча равишда, хусусий сектор технология гигантлари ва Украинанинг IT армияси Россиянинг киберҳужумларининг потенциал кўламини чекловчи омиллар бўлиб кўринади. Бироқ, АҚШ урушда бевосита иштирок этмасдан туриб, Украинани қўллаб-қувватлашда қанчалик узоққа бориши мумкинлиги очиқ савол бўлиб турибди.

Украинадаги урушнинг дастлабки бир неча ҳафталарида Россиянинг муҳим киберҳужумларининг йўқлигига сабаб бўлган омилларни санаб ўтиш учун вақт керак бўлади. Бироқ, агар далиллар Накасоннинг дастлабки даъвосини тасдиқласа (нафақат Украина, балки "бошқа" томонларнинг муваффақиятли кибермудофаа Россиянинг кибер таҳдидини камайтиришда муҳим рол ўйнади), у ҳолда АҚШ киберстратегиясининг келажаги учун иккита муҳим таъсир бор [16].

Биринчидан, кибермудофаа ва барқарорликка сармоя киритиш аҳмоқлик эмас, айниқса душманнинг кутилган ҳаракатларини кутиш. Иккинчидан, Қуролли кучлар тизимида киберхавфсизликни таъминлаш келажакда мудофаа концепциясининг бир қисми сифатида мавжуд халқаро ҳамкорликка асосланиш имкониятига эга бўлади. Ушбу масъулиятлар бир-бирини мустаҳкамлайди ва кутилаётган ҳимоя чоралари бошқа манфаатдор томонлар, айниқса рақибнинг кибер фаолияти билан яқинроқ ёки яхшироқ таниш бўлиши мумкин бўлган иттифоқчилар ва шериклар билан ишлашда юзага келадиган таҳдид муҳити ҳақида умумий тушунчани таъминлайдиган эрта огоҳлантиришга боғлиқ. Шу сабабли, Пентагоннинг киберстратегиясининг ҳужумкор жиҳатларига эътибор қаратилиши кибертаҳдидларни камайтиришда мудофаанинг асосий ролини яширади. Дарҳақиқат, мудофаа соҳасидаги ҳамкорлик келажакдаги мудофаа стратегияларида ҳал қилувчи омил бўлиб, Россиянинг Украинага аралашувидан сўнг унга устувор аҳамият берилиши керак.

Украинанинг аъзолигини ёқлаб овоз беришдан сўнг, Украина энди НАТОнинг Кибермудофаа билан ҳамкорликдаги мукаммаллик марказига қўшилади. Бу соҳада қадамлар қўйишда давом этар экан, Қўшма Штатлар ҳамкор давлатлар билан кўп томонлама ва икки томонлама шартномаларни институционализация қилиш ва бундай келишувларни киберстратегиянинг марказий ўрнига қўйиш орқали ҳамкорликка жиддий ёндашиши муҳим. Мудофаа фойдасига муҳит яратиш очиқ урушда кўринадиган беқарорлик шароитида барқарорликка олиб борадиган йўлдир.

Шу боисдан ҳам А.К.Расулев “Ёшларнинг ахборот-коммуникация маконига кенг жалб қилинганлиги, турли ҳуқуқбузарлик ва жиноятларни ўсмир-ёшлар томонидан содир этилаётганлигини инобатга олиб, ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятлар учун жиноий жавобгарлик ёшини 14 ёш, деб белгилаш мақсадга мувофиқ”[17 Б-23] деб таъкидлайди.

Бугунги кунга келиб Россиянинг Украинага ҳужуми барча жабҳаларда кучайди. Украина Россияга қарши қуруқликда, ҳавода ва Қора денгизда, шунингдек, кибермаконда курашмоқда. Украинада жисмоний ҳужумлар бошланиши билан кўпчилик киберҳужумлар ҳужумга тўғри келиши ёки ҳужумдан олдин бўлишини кутишган. Аммо ҳозирча кенг кўламли инфратузилма қулаши ёки ҳужумлар ҳақида хабар берилмаган. Аммо бу кибер фронт тинч дегани эмас.

Украина инқирозида энг илғор “фаол”дан тортиб то давлат идораларигача кибер-жанговарлар бошиданоқ иштирок этишди. Хабар қилинишича, ҳужумдан аввал россиялик хакерлар Украина ҳуқуқ-тартибот идоралари, телекоммуникациялар, давлат веб-сайтлари ва жамоат ташкилотларини чалкаштириб юбориш учун маълумотларни йўқ қилувчи HermeticWiper зарарли дастурдан фойдаланган. Шок ва қўрқув ҳужумларига келсак, бу кампаниянинг зарари сезиларли эди. Бунинг ҳақиқий сабаби номаълум. Владимир Путиннинг ҳужум қилиш ҳақидаги дастлабки режалари Байден маъмуриятининг разведка маълумотлари ёки АҚШ ёрдами сиздирилиши туфайли барбод бўлиши мумкин. Афтидан, Путин ва Россия кучлари украиналикларга ҳужум қила олишларига ҳаддан ташқари ишониб, бу воситаларни захирада сақламоқчи. Россиянинг A-Team келажакдаги эскалация сценарийларини кутаётган бўлиши мумкин. Бунинг ўрнига, Украина бир қатор DdoS ҳужумларига учради, бу эса баъзи жойларда интернет алоқаларини узиб қўйди, банк ва бошқа онлайн платформаларни вақтинча бўлса ҳам тўхтатди. Кейинчалик Оқ уй бу ҳужумларни оммавий равишда Россия разведкаси билан боғлади, аммо бу ўрта даражадаги ҳужумлар асосан қуйи даражадаги (асос) киберҳужумчиларнинг иши эди.

Украина кибер-ҳимоячилари DDoS ҳужумларининг дастлабки “олови”га бироз тайёр бўлиб туюлди. Трафикни бошқа тармоқ провайдерларига ўтказиш орқали Киев бу ҳужумларга анча чидамли эканлигини исботлади. Сўнгги кунларда Украинанинг энг кучли ҳужумга учраган қисмларида содир бўлган бошқа узилишлар киберҳужумлардан кўра кўпроқ инфратузилмани йўқ қилиш, аҳолини кўчириш ва электр станцияларини назорат қилиш билан боғлиқ. Дарҳақиқат, Украинадаги кибер урушда нафақат ҳукуматлар иштирок этмоқда. Kreml Conti тўлов гуруҳини фаол фаоллаштирди ва беларуслик хакерлар Украина ҳарбий нишонларига қарши фишинг кампаниясини ўтказаётгани хабар қилинди. Шу мақсадда Киев маҳаллий хакерларни мамлакатнинг муҳим инфратузилмасини ҳимоя қилишга ва Россия қўшинларига жосуслик қилишга чақирган. Украина бош вазири ўринбосари ва рақамли трансформация вазири Михаил Федоров телеграмм каналини яратди ва украиналиклар ёки хорижликлар учун Украина томонидаги курашга қўшилиш учун иш эълон қилди. Украинага хайрихоҳ хакерлар учун инглиз тилидаги такрорий реклама Россия корхоналари, банклари, Газпром каби ресурслар ишлаб чиқарувчи ташкилотлар ва ҳатто Россия ҳукумати веб-

сайтларини ўзларига хавф туғдириш учун “ҳар қандай кибер ёки DDoS ҳужумлари векторларидан” фойдаланишга ундайди.

Ҳатто машҳур “Anonymous” гуруҳи ҳам “Россия ҳукуматига қарши расман кибер урушда” эканини эълон қилиб, курашга қўшилди. Гуруҳнинг даъво қилишича, у Беларус қурол ишлаб чиқарувчиси Тетраедронни бузиб, Путин кучларига логистик ёрдам кўрсатиш эвазига 200 гигабайт электрон почтани ўғирлаган. Бундан ташқари, гуруҳ берган маълумотларга кўра, Россия оммавий ахборот воситалари Россия телевидениеси орқали кампаниянинг камчиликларини яшириш учун бузиб киришган ва фронт чизиғидан аниқ тасвирлар кўрсатган [18].

Ҳукумат ва нодавлат субъектларнинг киберможарога аралашуви бугунги ҳодиса, лекин ҳукумат вакиллари фуқаро хакерларни ўз мамлакатлари ишига ўз тезлигида қўшилишга очиқ рағбатлантириши турли даражадаги киберможаролар эволюцияси ва кучайиб бораётганидан далолат беради. Буни ҳақиқий кибер уруш деб аташ мумкин. Ўз навбатида “Глобал интернет тармоғидаги коммуникатив интернет жамоалар, яъни блоглар ва ижтимоий тармоқлар, норасмий миллий сегментнинг методологик ва методик муаммолари, бевосита шахс дунёқараши ва виртуал оламнинг диалектик қарама-қаршилигига боғлиқ. Бу жараёндаги асосий қийинчилик шундан иборатки, тадқиқотчи таҳлил давомида ижтимоий воқеликни кўзда тутсада, тадқиқот объекти виртуал дунё мазмуни ҳисобланади ва кўпгина ҳолларда аноним, билвосита характерга эга бўлади” [19 Б-16].

Киберможаролар авжига чиқар экан, давлат амалдорлари кибержамоаларни диққат билан кузатиб, ўзлари хоҳлаганча ҳаракат қилишларига шубҳа йўқ. Путин муҳим инфратузилма операторларига “компьютер ҳужумларидан” ҳушёр бўлишни буюрди. Байден маъмурияти худди шундай огоҳлантиришни маҳаллий компанияларга, айниқса мудофаа саноатига берди. Ҳозирча, икки кибер куч марказлари кескинлашув спиралидан қўрқиб, тўғридан-тўғри зарбаларга эриша олмаганга ўхшайди. Бироқ президент Жо Байден Путинни АҚШ компаниялари ва муҳим инфратузилмаларига киберҳужумлардан огоҳлантирди.

Бир нарса аниқ – Путин ҳар қандай йўл билан Киевни қўлга киритиш учун саъй-ҳаракатларини кучайтиради. Бир томондан, фуқаролар молотов коктейллари тайёрлаб, ҳукумат томонидан тақдим этилган қуролларни олмоқда, иккинчи томондан, ИИВ фуқароларни мобил қурилмаларида геолокация функцияларини ўчириб қўйишга чақирмоқда, чунки бу функция ёқилса, Россия кибержосуслари шаҳардаги ҳарбий йиғинларни аниқлаши мумкин бўлади.

2008 йилдан бери Қўшма Штатлардан разведка ва киберхавфсизлик бўйича мутахассислар маслаҳати билан БАА кибертехнологияда сезиларли ютуқларга эришди. Бу вақт мобайнида АҚШ номидан БААга киберхавфсизлик соҳасидаги етакчи экспертлардан бири ва АҚШнинг катта маслаҳатчиси Ричард Кларк юборилди. БААда кибертехнологиялар ташкилотини ташкил этиш учун Абу-Дабига келган Кларк Гуд Ҳарбор орқали Равен лойиҳаси деб номланувчи муҳим лойиҳани бошлагани маълум [20].

Равен лойиҳаси БААга баъзи ҳукуматлар, журналистлар ва ҳуқуқ ҳимоячиларини кузатишга ёрдам берадиган яширин ташаббус сифатида танилган. 2014 йилгача ушбу

муҳим лойиҳа Абу-Даби вилласида яширинча амалга оширилган ва АҚШ разведка ва хавфсизлик мутахассислари иштирокида ривожлана бошлаган. Лойиҳада БАА Қатар ва Эрон каби давлатларни нишонга олган кибер операцияларга эътибор қаратаётгани ва кибер жосуслик соҳасидаги технологик инфратузилмасини яхшилагани таъкидланган. Бундан ташқари, Равен ва БААда давлат томонидан ҳомийлик қилинган барча кибер-жосуслик операциялари 2014 йилнинг охирида ташкил этилгани тахмин қилинган Дарк Маттер билан бошлангани даъво қилинган. БААнинг собиқ миллий хавфсизлик маслаҳатчилари ва разведка ходимларини яратишдаги таъсири билан танилган Dark Matter БАА маъмуриятининг кибер-жосуслик дастурида муҳим “штаб-квартира” сифатида белгиланиши мумкин [21].

Технологик имкониятларини мухолиф унсурларга босим ўтказиш воситаси сифатида ишлатган Абу Даби ҳукумати, разведка соҳасида хорижий давлатлар ва компаниялар билан ҳамкорлик қилиб, кибер қурол савдосига аҳамият бераётганини кўриш мумкин. Шу муносабат билан, 2011-2016 йиллар давомида БАА “миллий хавфсизлик, терроризм ва ноқонуний фаолиятга қарши кураш” учун Италиянинг HackingTeam, Германиянинг FinFisher ва Исроилнинг NSO каби компанияларидан технологик жосуслик воситаларини харид қилган. Масалан, 2011-йилда чоп этилган техник ҳужжатларга кўра, БАА журналисти ва фаоли Аҳмад Мансур ҳибсга олинишидан аввал FinFishernинг мобил телефонига юборилган FinSpy киберқуроли ёрдамида БАА разведкаси томонидан кузатилган.

2016-йилда БАА бугунги киберқурол саноатининг асосий ўйинчиси сифатида таърифланиши мумкин бўлган NSO етакчи маҳсулоти Пегасус орқали мухолифат вакиллари, журналистлар ва фаоллар устидан жосуслик қилаётгани аниқланган. Дунёдаги энг кучли ва мураккаб кибер-жосуслик қурилмаларидан бири сифатида танилган Pegasus БААга қачон ва ким орқали сотилгани баҳсли. Ўша йилларда Исроил билан дипломатик алоқалари суст бўлган БАА Исроил разведкаси орқали миллионлаб долларлик қурол сотиб олгани айтилади.

Маълумки, БАА ва бошқа барча хорижий мамлакатларга сотиладиган кибертехнологиялар ёки бошқа мудофаа/хавфсизлик маҳсулотлари Исроил маъмурияти томонидан тасдиқланиши керак. Эслатиб ўтамиз, Исроилнинг кибертехнология компаниялари томонидан ишлаб чиқилган кибержосуслик ва кузатув воситалари Исроил Мудофаа вазирлиги рухсати билан хорижга ҳам сотилиши мумкин. NSO, Cellebrite ва Verint каби киберқурол компаниялари ҳам хорижий разведка хизматлари билан махфий / очиқ шартномалар тузишлари мумкин.

Бу ерда баъзи Исроил кибертехнология компаниялари маҳсулотларига оид яна бир қизиқ жиҳатни таъкидлаш керак. Айрим ҳолларда тегишли компаниялар томонидан ишлаб чиқарилган кибертехнологиялар мумкин бўлган разведка ва хавфсизлик муаммолари туфайли маълум мамлакатларда фаол бўлмаслиги мумкин. Масалан, дунёнинг кўплаб разведка хизматлари ва ҳуқуқ-тартибот идоралари томонидан сотиб олинган NSOнинг Pegasus кибер қуроли Исроил, АҚШ, Россия, Хитой ва Эронда ишламайди. Мобил телефонида NSO жосуслик дастурини сиздирган шахс юқорида тилга олинган мамлакатлардан бирининг чегарасига кирган пайтдан бошлаб, дастур GPS идентификацияси орқали ўчирилади.

Яқин Шарқни кибертехнология воситалари билан таъминловчи Исроилдан ташқари, БААда АҚШ разведка идоралари ҳам таъсирчан эканлиги маълум. Қўшма Штатлар БАА маъмуриятига, хусусан, Миллий хавфсизлик агентлиги (NSA) ва баъзи компаниялар орқали киберхавфсизлик ечимлари/воситалари орқали техник ёрдам кўрсатади деган даъволар мавжуд. Шу муносабат билан, масалан, DarkMatter ва БАА Исроилнинг собиқ Unit8200 ҳарбий разведка бўлинмаси ва АҚШдаги НСА ходимларини жуда юқори маош эвазига ишга олгани маълум бўлди. Ушбу ҳамкорликнинг бир қисми сифатида Dark Matter нинг бозор қиймати 500 миллион доллардан ортиқ бўлган кибер истеъдод ва технологик разведка қобилиятлари ривожлана бошлади. Натижада, БАА маъмуриятининг ўз чегараларидаги кибер-жосуслик ва кузатув қобилиятлари шахсий дахлсизликнинг мумкин бўлган бузилиши нуқтаи назаридан ташвишли даражага етди [22].

Хулоса ва таклифлар (Conclusion/Recommendations). Биринчидан, бугунги кунда ҳарбий кучнинг халқаро муносабатлар омили сифатидаги аҳамияти сақланиб қолмоқда ва айрим ҳолларда ҳатто ортиб бормоқда. Шу билан бирга, ахборот инқилоби ва ҳарбий ишларда инқилоб давом этмоқда. Шу сабабли, ахборот технологиялари таъсирида ҳарбий соҳада содир бўлаётган ўзгаришлар катта тадқиқот учун қизиқиш уйғотади.

Иккинчидан, ушбу мавзу бўйича нашрларнинг кўплигига қарамай, келажакдаги қуролли тўқнашувларда ахборот технологияларининг ўрни билан боғлиқ кўплаб муаммолар ҳали ҳам ўрганилмаган. Ҳарбий ишларда ахборот технологияларининг роли ва ўрни ҳақидаги саволнинг ўзи баъзан мутахассисларнинг қарама-қарши фикрларни келтириб чиқаради.

Учинчидан, етакчи давлатларнинг ҳарбий стратегияларида ахборот технологияларининг ўрни ва қуролли можароларда ахборот технологияларидан фойдаланиш тажрибасини ўрганиш зарур. Бундан ташқари, бу борадаги бир қанча давлатларнинг тажрибасини ўрганиш мақсадга мувофиқ кўринади, чунки баъзи давлатлар ахборот технологияларини ҳукмронлик мавқеини сақлаб қолиш усуллари ва воситалари, бошқалари эса – сиёсий таъсирни ошириш йўллари сифатида кўришади.

Тўртинчидан, етакчи давлатларнинг ҳарбий-сиёсий раҳбарияти ва экспертлари ҳарбий ишларда ахборот технологияларидан фойдаланиш муаммоси билан боғлиқ бир қатор асосий тушунчаларни (хусусан, “кибертаҳдид”, “киберхавфсизлик”) қандай изоҳлашини тушуниш муҳимдир.

Бешинчидан, ахборот инқилоби таъсирида замонавий қуролли тўқнашувлар табиати ҳамда етакчи давлатларнинг ҳарбий-сиёсий раҳбарияти ва экспертларининг ҳарбий сиёсатнинг мақсад ва воситаларига қарашлари қандай ўзгариб бораётганини ўрганиш зарур.

Олтинчидан, қуролли можароларда ахборот технологияларидан фойдаланишнинг халқаро сиёсий оқибатларини таҳлил қилиш мамлакатимизда ҳарбий қурилишнинг устувор йўналишларини аниқлаш имконини беради.

References:

1. Мирзиёев Ш. Миллий тараққиёт йўлимизни қатъият билан давом эттириб, янги босқичга кўтарамиз. 1-жилд. “Ўзбекистон”, 2017. – Б. 27.;
2. https://www.kuow.org/stories/william-gibson-coining-word-cyberspace/.;
3. https://www.tandfonline.com/doi/full/10.1080/23265507.2015.1084477.;
4. https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%8.;
5. Хайдаров К.А. Мудофаа тизимида ахборотнинг психологик хавфсизлигини таъминлаш механизми (очиқ манбалар мисолида). Сиёсий фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати. – Тошкент-2020. –Б.5.;
6. https://www.nytimes.com/1988/11/05/us/author-of-computer-virus-is-son-of-nsa-expert-on-data-security.html.;
7. https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia.;
8. Раҳмон Қўчқор. Дунё кураш майдонидир//. – Тафаккур-2016. 4-сон Б. 24.
9. Сэрра Э. Кибербезопасность: правила игры : как руководители и сотрудники влияют на культуру безопасности в компании:Эллисон Сэрра ; перевод с английского: Людмила Смилевска. - Москва : Альпина ПРО, 2021. - 181 с.; Паренти Т. Кибербезопасность. Что руководителям нужно знать и делать. - Москва : Манн, Иванов и Фербер, 2021. Тронкон П. Bash и кибербезопасность: атака, защита и анализ из командной строки Linux: / Пол Тронкон, Карл Олбинг ; [пер. с англ. А. Герасименко]. - Санкт-Петербург [и др.] : Питер, 2020. - 285 с.;
10. Сафронова И.Л. Политические проблемы обеспечения международной информационной безопасности : диссертация ... кандидата политических наук. - Москва, 2006. - 211 с.; Соловьева Е.А. Информационное противоборство в сети Интернет: политологический анализ: диссертация...кандидата политических наук. - Пятигорск, 2011. - 215 с.;
11. Ўзбекистон Республикасининг “Ахборотлаштириш ва маълумотлар узатиш соҳасида қонунга хилоф ҳаракатлар содир этганлик учун жавобгарлик кучайтирилганлиги муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида” 2007 йил 25 декабрдаги ЎРҚ–137-сон Қонуни // lex.uz – Ўзбекистон Республикаси Қонун ҳужжатлари маълумотлари миллий базаси // Рустамбаев М.Х. Ўзбекистон жиноят қонунчилиги: яратилиши тарихи, бугунги куни, ривожланиши истиқболлари. – Т.: Адолат, 2017 й., http://old.adolatnashr.uz. Рустамбоев М.Х. Ўзбекистон Республикаси жиноят ҳуқуқи курси. IV том. Махсус қисм. “Илм-зиё” нашриёт уйи. 2011 й. – Б.56.; Рустамбоев М.Х. Ўзбекистон Республикасининг Жиноят кодексига шарҳ. Махсус қисм. – Т.: “Адолат” нашриёти. 2016 й., 861-бет.; Самаров Р. Вооруженные силы гарант безопасности страны и стабильности в регионе // Ўзбекистон Республикаси Қуролли Кучларининг тарихи, бугуни ва келажаги // Республика илмий-амалий анжуман материаллари. – Тошкент: МВ, 2005. – Б. 226-229.;
12. https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8_%D0%A1%D0%A8%D0%90.;

13. https://cyberleninka.ru/article/n/o-podhodah-rukovodstva-knr-i-kitayskih-silovyh - struktur-k-protivoborstvu-v-kiberprostranstve.;
14. https://www.avnrf.ru/index.php/publikatsii-otdelenij-avn/nauchnykh-otdelenij / voennogo-iskusstva/59-vojna-budushchego-prognosticheskij-analiz.;
15. https://naked-science.ru/article/tech/voyna-budushchego.;
16. https://www.rand.org/search.html?query=cyber+security.;
17. Расулев А.К. Ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятларга қарши курашишнинг жиноят-ҳуқуқий ва криминологик чораларини такомиллаштириш. Докторлик (DSc) диссертацияси автореферати. –Тошкент, 2018. – Б.23.;
18. https://6park.news/louisiana/how-the-ukraine-conflict-is-reshaping-the-dark-web.html.;
19. Бурханов Х.М. Интернет хавфсизлигини таъминлашда миллий сегмент фаолиятининг социологик жиҳатлари. Социология фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати. - Тошкент– 2021. –Б.16.;
20. https://www.reuters.com/article/us-usa-raven-whitehouse-specialreport id USK BN1YE1OB.;
21. https://en.wikipedia.org/wiki/DarkMatter_(company).;