E CONF SERIES

International Conference on Modern Science and Scientific Studies
Hosted online from Madrid, Spain
Website: econfseries.com 20th May 2025

ZAMONAVIY URUSHLAR MAYDONI: KIBERHUDUDLAR VA DAVLATLARARO RAQAMLI TO‘QNASHUVLAR

Shernazarov Elbek Ilhomovich
Buxoro viloyati Peshku tumani ichki ishlar bo‘limi boshlig‘i podpolkovnik

ANNOTATSIYA

Zamonaviy urushlar maydoni an’anaviy jang maydonlaridan farqli o‘laroq, kiberhududlarda ham davom etmoqda. Davlatlararo raqamli to‘qnashuvlar axborot texnologiyalari orqali siyosiy, iqtisodiy va harbiy maqsadlarni amalga oshirish uchun yangi imkoniyatlar yaratadi. Kiberxavfsizlik, kiberhujumlar va raqamli razvedka vositalari orqali davlatlar o‘zaro raqobat olib boradi. Ushbu maqolada kiberhududlardagi raqamli to‘qnashuvlarning xususiyatlari, ularning zamonaviy urushlardagi roli va davlatlararo raqobatdagi ahamiyati tahlil qilinadi.

Kalit so‘zlar: zamonaviy urushlar, kiberhudud, raqamli to‘qnashuvlar, kiberxavfsizlik, davlatlararo raqobat, kiberhujumlar, raqamli razvedka, axborot texnologiyalari.

Kiberhududlar davlatlararo raqamli to‘qnashuvlar maydoni sifatida siyosiy strategiyalarni yangi bosqichga olib chiqmoqda. Endi urushlar faqat fiziki jang maydonida emas, balki axborot tarmoqlarida ham kechadi, bu esa davlatlar uchun kiberxavfsizlikni ustuvor vazifa sifatida belgilaydi.

Raqamli razvedka vositalari yordamida davlatlar raqiblarining ichki axborot tizimlariga kirib, strategik ma’lumotlarni yig‘ish va ta’sir o‘tkazish imkoniga ega bo‘lmoqda. Bu esa zamonaviy urushlarning samaradorligini oshiradi hamda yangi xavf-xatarlarni keltirib chiqaradi.

Kiberhujumlar yordamida iqtisodiy infratuzilmalarni va moliyaviy tizimlarni zaiflashtirish mumkin. Shunday qilib, davlatlar o‘zaro to‘qnashuvlarda iqtisodiy barqarorlikni buzish orqali raqiblarini siyosiy jihatdan sustlashtirishga harakat qiladi.

Davlatlararo raqamli raqobat sharoitida kiberxavfsizlik sohasi mutaxassislarini tayyorlash va ularni doimiy ravishda malakasini oshirib borish muhimdir. Harbiy va

fuqarolik sektorida yangi kiberhujumlarga qarshi tezkor javob berish tizimlari tashkil etilishi zarur.

Axborot texnologiyalari tez sur'atlarda rivojlanayotgani sababli, kiberhududlarda yuzaga keladigan yangi tahdidlarni oldindan aniqlash va ularni bartaraf etish uchun davlatlar o'rtasida hamkorlik va axborot almashinuvi muhim ahamiyat kasb etadi.

Shuningdek, davlatlararo raqamli to'qnashuvlar qonuniy va axloqiy chegaralarni qayta ko'rib chiqishga majbur qilmoqda, chunki kiberurushlar natijasida tinch aholiga yetadigan zararlar va global xavfsizlikka ta'sirlar ortib bormoqda.

Zamonaviy urushlar va kiberhududlarda raqamli himoya tizimlarini kuchaytirish orqali davlatlar o'z suverenitetini himoya qilishi va yangi texnologik raqobat maydonida o'z o'rnini mustahkamlashi mumkin.

Davlatlar kiberhujumlarni oldini olish uchun maxfiy axborot tizimlarini muntazam yangilab, xavfsizlik devorlarini (firewall) kuchaytirish bilan shug'ullanadi. Bu usul raqamli hujumlarning muvaffaqiyatga erishish ehtimolini kamaytiradi.

Axborot razvedkasi agentliklari raqamli tarmoqlardagi soxta ma'lumotlar va firibgarliklarni aniqlash uchun sun'iy intellekt va katta ma'lumotlarni tahlil qilish texnologiyalaridan foydalanadi. Bu kiberurushlarni oldindan aniqlash va ularga qarshi choralar ko'rishga imkon beradi.

Davlatlararo raqamli to'qnashuvlarda zarar ko'rgan infratuzilmalarning tezda tiklanishi uchun favqulodda vaziyatlar uchun rejalashtirilgan zaxira tizimlari va muqobil ma'lumot markazlari tashkil qilinadi.

Kiberxavfsizlik sohasida malakali kadrlarni tayyorlash uchun maxsus o'quv markazlari ochilib, ular kiberhujumlarga qarshi real vaqt rejimida kurashish bo'yicha amaliy treninglar o'tkazadi. Bu yondashuv mamlakatning raqamli xavfsizligini mustahkamlashga xizmat qiladi.

Tashqi davlatlardan keladigan kiberhujumlarga qarshi maxsus monitoring markazlari faoliyat yuritadi, ular raqamli faoliyatni doimiy kuzatib, har qanday xavfli harakatlarni tezda aniqlaydi va bloklaydi.

Xalqaro hamkorlik doirasida kiberxavfsizlik bo'yicha kelishuvlar va bitimlar imzolanadi, bu esa davlatlararo raqamli to'qnashuvlarning oldini olish va ularni nazorat qilish imkonini yaratadi.

Davlatlar o‘z milliy kiberxavfsizlik strategiyalarini ishlab chiqib, unda harbiy, fuqarolik va biznes sektori o‘rtasida hamkorlikni mustahkamlash orqali kiberhujumlarga qarshi umumiy mudofaa tizimini shakllantiradi.

Axborot texnologiyalari sohasida tezkor yangiliklarni doimiy kuzatib borish orqali yangi xavf-xatarlar paydo bo‘lishini oldindan bashorat qilish va ularga tayyor turish mumkin.

Zamonaviy urushlar va kiberhududlar mavzusidan kelib chiqqan holda, faqat amaliy jihatdan yoritilgan kreativ misollarni jadval shaklida taqdim etaman:

Amaliy Yo‘nalish	Misol va Tavsif
Kiberinfratuzilmani himoya qilish	Davlat muhim axborot tizimlarini muntazam yangilab, xavfsizlik devorlari va shifrlash usullarini kuchaytiradi.
Kiberrazvedka faoliyati	Sun’iy intellekt yordamida tarmoqlardagi noxush faoliyatlarni aniqlash va xakerlik hujumlarini oldini olish.
Favqulodda holatlar uchun rejalashtirish	Zararlangan tizimlarni tiklash uchun zaxira serverlar va muqobil ma’lumot markazlari tashkil etish.
Mutaxassislarni tayyorlash	Kiberxavfsizlik bo‘yicha amaliy treninglar va malaka oshirish kurslari tashkil etiladi.
Real vaqt monitoring	Maxsus markazlarda raqamli trafik doimiy kuzatiladi va xavfli harakatlar darhol aniqlanadi.
Xalqaro hamkorlik	Kiberxavfsizlik bo‘yicha davlatlararo kelishuvlar tuzilib, kiberhujumlarga qarshi birgalikda harakat qilinadi.
Milliy strategiyalar yaratish	Harbiy, fuqarolik va biznes sektori o‘rtasida umumiy kiberxavfsizlik tizimi ishlab chiqiladi va amalga oshiriladi.
Innovatsiyalar va monitoring	Yangi xavflarni aniqlash uchun zamonaviy texnologiyalar va axborot tizimlari doimiy ravishda yangilanadi.

Energetika tizimlariga hujumlar. Bir davlatning elektr tarmoqlariga kiberhujum uyushtirilib, ko‘plab shaharlarda elektr energiyasi uzilib qoldi. Bu holat nafaqat fuqarolarning kundalik hayotiga ta’sir qilgani, balki sanoat korxonalarining ishini to‘xtatishiga olib keldi. Bunday hujumlar infratuzilmaning zaif tomonlarini ko‘rsatib, mamlakatni iqtisodiy jihatdan zaiflashtirishga qaratilgan.

Moliyaviy tizimlarga zarar yetkazish. Davlatlararo kiberurushlarda bank tizimlariga nishon qilingan xakerliklar ko‘paymoqda. Masalan, bir bankning asosiy serverlariga hujum qilinib, mijozlarning hisob raqamlaridan katta miqdorda pul o‘g‘irlandi. Bu moliyaviy tizimga bo‘lgan ishonchni pasaytirib, xalqaro moliyaviy bozorlarga ham salbiy ta’sir ko‘rsatadi.

Axborot urushlari va manipulyatsiya. Muayyan davlatlar o‘z manfaatlarini ilgari surish uchun ijtimoiy tarmoqlarda soxta yangiliklar tarqatadi, odamlarning fikrini boshqaradi. Bu jarayon siyosiy beqarorlikni kuchaytirib, ijtimoiy ziddiyatlarni oshiradi. Misol uchun, saylov oldidan keng miqyosda soxta ma’lumotlar tarqatilib, saylov natijalariga ta’sir ko‘rsatishga urinishlar bo‘ladi.

Sun’iy intellekt bilan ishlovchi himoya tizimlari. Kelajakda raqamli to‘qnashuvlarda avtomatlashtirilgan sun’iy intellekt tizimlari qo‘llaniladi. Ushbu tizimlar kiberhujumlarni real vaqt rejimida aniqlab, avtomatik tarzda bloklaydi. Misol uchun, bankning onlayn tizimi sun’iy intellekt yordamida shubhali harakatlarni sezib, darhol bloklash mexanizmini ishga tushiradi.

2015-yil, Ukraina energetika tizimiga kiberhujum. Ukrainaning elektr ta’minoti tizimiga uyushtirilgan kiberhujum natijasida minglab uylar va korxonalar bir necha soat davomida elektrsiz qolgan. Bu hodisa infratuzilmaning raqamli zaifliklarini ko‘rsatdi va davlatlararo kiberurushlar yangi bosqichga ko‘tarilganini namoyish etdi.

2017-yil, WannaCry ransomware hujumi. Dunyodagi ko‘plab davlatlarning sog‘liqni saqlash, transport va boshqa sohalarida tizimlar shifrlab qo‘yilib, katta zarar yetkazildi. Ushbu hujum global kiberxavfsizlik muammolarining dolzarbligini yana bir bor ko‘rsatdi va davlatlarni himoya tizimlarini mustahkamlashga undadi.

2016-yil, AQSh saylovlariga aralashish. AQSh prezidenti saylovlari oldidan Rossiya tomonidan ijtimoiy tarmoqlarda soxta yangiliklar va manipulyatsiyalar

tarqatilgan. Bu jarayon davlat siyosatiga bevosita ta’sir ko‘rsatishga qaratilgan raqamli urushning bir qismi sifatida qaraldi.

2020-yil, Sun’iy intellekt yordamida kiberhujumlar. Ba’zi davlatlarning xavfsizlik agentliklari sun’iy intellekt algoritmlaridan foydalangan holda kiberhujumlarni aniqlash va bloklash bo‘yicha ilg‘or tizimlar yaratdi. Bu texnologiya kiberxavfsizlik sohasida inqilobiy o‘zgarishlarga sabab bo‘lmoqda.

Kelajakdagi prognozlar: 2030-yilga kelib kvant shifrlash texnologiyalari Mutaxassislar kvant hisoblash texnologiyalarining rivojlanishi bilan hozirgi shifrlash usullari eskirishi, yangi kvantga chidamli himoya tizimlari keng joriy etilishi kutilmoqda. Bu esa davlatlararo raqamli urushlarda yangi himoya qatlamlarini yaratishga imkon beradi.

XULOSA

Zamonaviy urushlar maydoni kiberhududlarga ko‘chib, davlatlararo raqamli to‘qnashuvlar yangi xavf va imkoniyatlarni yuzaga keltirmoqda. Kiberxavfsizlik davlat suverenitetini himoya qilishda muhim omilga aylangan bo‘lib, raqamli infratuzilmalarning himoyasi va axborot razvedkasi orqali raqiblarning hujumlarini oldini olish imkonini beradi. Davlatlararo hamkorlik va milliy strategiyalarni shakllantirish orqali kiberhujumlarga qarshi samarali kurash olib borish mumkin. Shu bilan birga, kiberxavfsizlik sohasidagi malakali kadrlarni tayyorlash va zamonaviy texnologiyalarni doimiy ravishda yangilab borish — raqamli to‘qnashuvlarda muvaffaqiyatga erishishning kalitidir. Natijada, kiberhududlarda yuzaga kelayotgan tahdidlarni kamaytirish va zamonaviy urushlarning yangi shakllariga qarshi samarali javob qaytarish imkoniyati yaratiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. To‘xtaboyev, A. Kiberxavfsizlik asoslari va amaliyoti. Toshkent, 2021.
2. Rasulov, B. Axborot xavfsizligi va raqamli texnologiyalar. Toshkent, 2020.
3. Islomov, M. Davlat kiberxavfsizligi va zamonaviy tahdidlar. Toshkent, 2022.
4. Karimova, N. Internet va kiberxavfsizlik: nazariya va amaliyot. Toshkent, 2019.