KIBERMAKONDA KUCHLAR MUVOZANATI MUAMMOLARI VA UNING XALQARO XAVFSIZLIKKA TA'SIRI

Qurbonova Xusnora Doniyor qizi
Jahon iqtisodiyoti va diplomatiya universiteti Xalqaro munosabatlar fakulteti 1-bosqich talabasixusnoraqurbonova6@gmail.com

Annotatsiya: *Ushbu maqolada kibermakonda kuchlar muvozanati muammolari va uning xalqaro xavfsizlikka ta'siri tahlil qilingan. Maqolada kibermakonning zamonaviy xalqaro munosabatlardagi o'rni, undagi kuch tushunchasining o'ziga xos xususiyatlari hamda an'anaviy kuchlar muvozanati modelining raqamli muhitga moslashishdagi cheklovlari yoritilgan. Shuningdek, kibermakonda kuchni o'lchashning murakkabligi, atributsiya muammosi, asimmetrik imkoniyatlar va nodavlat aktorlarning ortib borayotgan roli kabi asosiy muammolar tahlil qilingan. Mavjud dalillar asosida kibermakonning real infratuzilmalar va global iqtisodiyotga ta'siri ko'rsatib berilgan. Maqolada xalqaro xavfsizlik tizimida yuzaga kelayotgan yangi tahdidlar va ularni bartaraf etish yo'llari, jumladan, xalqaro hamkorlikni kuchaytirish, huquqiy normalarni rivojlantirish va kiber-diplomatiyani takomillashtirish zarurligi asoslab berilgan.*

Kalit so'zlar: *kibermakon, kuchlar muvozanati, xalqaro xavfsizlik, attributsiya muammosi, assimetrik imkoniyatlar, kiber-diplomatiya, Tallinn Manual.*

Аннотация: *В данной статье анализируются проблемы баланса сил в киберпространстве и его влияние на международную безопасность. В исследовании рассматриваются роль киберпространства в современных международных отношениях, специфические особенности понятия силы в данной сфере, а также ограничения адаптации традиционной модели баланса сил к цифровой среде. Кроме того, анализируются ключевые проблемы, такие как сложность измерения силы в киберпространстве, проблема атрибуции, асимметричные возможности и растущая роль негосударственных акторов. На основе имеющихся данных показано влияние киберпространства на критическую инфраструктуру и мировую экономику. В статье также обосновывается необходимость реагирования на возникающие угрозы в системе международной безопасности, включая укрепление международного сотрудничества, развитие правовых норм и совершенствование кибердипломатии.*

Ключевые слова: *киберпространство, баланс сил, международная безопасность, проблема атрибуции, асимметричные возможности, кибердипломатия, таллиннское руководство.*

Abstract. *This article analyzes the problems of the balance of power in cyberspace and its impact on international security. The study highlights the role of cyberspace in contemporary international relations, the specific features of the concept of power within it, and the limitations of adapting the traditional balance of power model to the digital environment. It also examines key issues such as the complexity of measuring power in cyberspace, the attribution problem, asymmetric capabilities, and the growing role of non-state*

actors. Based on existing evidence, the impact of cyberspace on critical infrastructures and the global economy is demonstrated. The article further substantiates the need to address emerging threats in the international security system, including strengthening international cooperation, developing legal norms, and improving cyber diplomacy.

Key words: *cyberspace, balance of power, international security, attribution problem, asymmetric capabilities, cyber diplomacy, Tallinn Manual.*

KIRISH

Kibermakon - bu internet, kompyuter tizimlari va boshqa raqamli texnologiyalar orqali yaratilgan virtual muhit bo‘lib, unda ma’lumotlar uzatiladi, saqlanadi va foydalanuvchilar o‘zaro aloqada bo‘ladi.[31] U real dunyoga bevosita ta’sir ko‘rsatadigan muhim global makon hisoblanadi. Bugungi kunda kibermakon zamonaviy xalqaro tizimda tobora muhim ahamiyat kasb etib, ko‘plab tadqiqotchilar tomonidan “beshinchi jang maydoni” sifatida e’tirof etilmoqda.[32] An’anaviy jang maydonlari - quruqlik, dengiz, havo va kosmosdan farqli ravishda, u chegaralarsiz, yuqori darajada dinamik va murakkab muhitdir.

Davlatlar, nodavlat aktorlar va individual subyektlarning ushbu makondagi faoliyati global xavfsizlik muammolarini yanada murakkablashtirmoqda. Shu sababli, kibermakonning strategik ahamiyati ortib borib, xalqaro munosabatlarning ajralmas qismiga aylanmoqda.

Biroq, kibermakonda kuchlar muvozanatini aniqlash va uni saqlash an’anaviy harbiy kuchlarga nisbatan ancha mushkuldir. Chunki bu sohada kuchni o‘lchash mezonlari aniq emas, hujum manbasini aniqlash qiyin va javob choralarining chegaralari noaniq. Natijada, bu holat davlatlar o‘rtasida ishonchsizlikni kuchaytirib, kutilmagan nizolar yuzaga kelishiga olib kelishi mumkin.

Kibermakon zamonaviy xalqaro munosabatlar tizimida an’anaviy geosiyosiy makonlardan tubdan farq qiluvchi yangi muhit sifatida shakllanmoqda. Ushbu makonda kuch tushunchasi klassik harbiy yoki iqtisodiy resurslarga emas, balki texnologik ustunlik, axborot oqimlari ustidan nazorat hamda raqamli tizimlarga kirish va ularni boshqarish salohiyatiga asoslanadi. [33]Shu bois kibermakon kuchni qayta talqin qiluvchi va uni yangi mezonlar asosida belgilovchi strategik maydonga aylanmoqda. Kibermakondagi kuchning muhim xususiyatlaridan biri uning asimmetrik tabiatidir.[34] Ya’ni, resurslari cheklangan davlatlar yoki hatto nodavlat aktorlar ham nisbatan kam xarajat evaziga global miqyosda sezilarli ta’sir ko‘rsatish imkoniga ega. Bu esa an’anaviy kuch ierarxiyasini zaiflashtirib, yangi aktorlarning paydo bo‘lishiga olib keladi.

Umuman olganda, kibermakondagi kuch quyidagi to‘rtta asosiy omil bilan belgilanadi: birinchidan, texnologik salohiyat darajasi; ikkinchidan, kiberinfratuzilma ustidan nazorat; uchinchidan, yuqori malakali inson kapitalining mavjudligi; to‘rtinchidan esa, ushbu resurslardan foydalanishga qaratilgan siyosiy iroda. Nazariy yondashuvlar nuqtai nazaridan,

[31] “Cyber Power” by Joseph Nye
[32] https://researchcorridor.org/index.php/ijcnw/article/view/521
[33] “The future of power” by Joseph Nye
[34] https://www.nature.com/articles/s41599-025-04897-7

kibermakon turli xalqaro munosabatlar maktablarining qarama-qarshi qarashlari chorrahasida joylashgan. Realistik yondashuv kibermakonni davlatlar o‘rtasidagi raqobat maydoni va “kiber qurollanish poygasi”ning yangi bosqichi sifatida talqin qiladi. Liberalizm esa aksincha, xalqaro institutlar va kooperatsiya mexanizmlari orqali bu makonda barqarorlikka erishish mumkinligini ta’kidlaydi.

Konstruktivistik yondashuv esa umumiy qoidalar va xulq-atvor normalarining yetishmasligi tufayli yuzaga kelayotgan noaniqlik va beqarorlikka urg‘u beradi.Shu bilan birga, yuqori darajadagi yashirinlik, vositalarning ikki tomonlama xususiyati va “plausible deniability” fenomeni sababli an’anaviy kuchlar muvozanati modeli bu makonda to‘liq ishlamaydi.[35] Natijada, kibermakon xalqaro xavfsizlik va barqarorlikka oid mavjud nazariy yondashuvlarni qayta ko‘rib chiqishni talab etadi. Kibermakonda kuchlar muvozanati muammolari Kibermakonda kuchlar muvozanatini ta’minlash masalasi zamonaviy xalqaro tizimdagi eng murakkab muammolardan biri hisoblanadi. An’anaviy harbiy muvozanatdan farqli ravishda, bu sohada kuchning tabiati noaniq, o‘zgaruvchan va ko‘p qatlamlidir.

Shu sababli, davlatlar o‘rtasida barqaror muvozanatni saqlash ancha qiyinlashadi. Birinchi asosiy muammo - kuchni o‘lchashning murakkabligi. An’anaviy tizimda davlat kuchi harbiy byudjet, qo‘shin soni yoki qurol-aslaha bilan baholanadi. Kibermakonda esa bunday aniq mezonlar mavjud emas. Davlatning haqiqiy kiber salohiyati ko‘pincha maxfiy bo‘lib, uning imkoniyatlari faqat amaliy hujum yoki mudofaa jarayonida namoyon bo‘ladi. Natijada, davlatlar bir-birining real salohiyatini to‘liq baholay olmaydi, bu esa noto‘g‘ri strategik qarorlar qabul qilinishiga olib kelishi mumkin. Ikkinchi muammo - atributsiya (hujum manbasini aniqlash) masalasi. Kibermakonda hujumni kim amalga oshirganini aniq isbotlash juda qiyin. Hujumlar ko‘pincha boshqa davlat hududi orqali yoki yashirin tarmoqlar yordamida amalga oshiriladi. Bu esa javob choralarini qo‘llashni murakkablashtiradi.

Misol sifatida, NotPetya 2017-yilda sodir bo‘lgan eng yirik kiberhujumlardan biri bo‘lib, u global miqyosda kompaniyalar va infratuzilmalarga katta zarar yetkazdi. Hujum natijasida umumiy iqtisodiy zarar taxminan 10 milliard dollarga baholanib, ayniqsa Maersk kabi yirik kompaniyalar faoliyati izdan chiqdi.[36] Dastlab virus sifatida ko‘ringan bu hujum aslida ma’lumotlarni tiklab bo‘lmaydigan tarzda yo‘q qilishga qaratilgan edi. Kiberxavfsizlik ekspertlari uni ko‘pincha Rossiya bilan bog‘lashadi, biroq bu rasmiy va to‘liq isbotlanmagan. Shu bois NotPetya hodisasi kibermakonda atributsiya muammosi, ya’ni hujum ortida kim turganini aniq belgilash qanchalik murakkab ekanining yaqqol misoli hisoblanadi.

Uchinchi muammo - asimmetrik imkoniyatlar mavjudligi. Kibermakonda kichik davlatlar yoki hatto nodavlat aktorlar ham katta davlatlarga jiddiy zarar yetkazishi mumkin. Buning uchun ularga katta harbiy resurslar emas, balki yuqori texnologik bilim va malaka yetarli bo‘ladi. Bu holat an’anaviy kuchlar muvozanati modelini izdan chiqaradi, chunki kuch nisbati har doim ham davlat hajmi yoki iqtisodiy qudratiga bog‘liq emas. To‘rtinchi muammo - nodavlat aktorlar rolining ortishi. Xakerlik guruhlari, xususiy

[35] https://www.sciencedirect.com/science/article/abs/pii/S187454821400002X
[36] https://www.hypr.com/security-encyclopedia/notpetya

kompaniyalar va hatto individual shaxslar ham kibermakonda muhim o‘yinchilarga aylangan.

Ularning faoliyati ko‘pincha davlat siyosatidan mustaqil bo‘lib, ba’zan esa davlatlar tomonidan bilvosita qo‘llab-quvvatlanadi. Bu esa javobgarlik va nazorat masalalarini yanada murakkablashtiradi. Beshinchi muammo - xalqaro huquqiy bazaning yetarli emasligi. Kibermakonda davlatlarning xatti-harakatlarini tartibga soluvchi aniq va majburiy xalqaro qoidalar to‘liq shakllanmagan. Mavjud normalar ko‘pincha umumiy xarakterga ega bo‘lib, ularni amaliyotda qo‘llash qiyin. Natijada, davlatlar o‘z manfaatlaridan kelib chiqib harakat qiladi, bu esa global darajada beqarorlikni kuchaytiradi. Yuqoridagi omillar yig‘indisi kibermakonda klassik “kuchlar muvozanati” modelining samarali ishlashiga to‘sqinlik qiladi. Natijada, davlatlar o‘rtasida strategik noaniqlik kuchayadi, bu esa kutilmagan nizolar va mojarolar yuzaga kelish ehtimolini oshiradi. Shuning uchun kibermakonda muvozanatni ta’minlash uchun yangi yondashuvlar va moslashuvchan mexanizmlar zarur.

Kibermakonda kuchlar muvozanatining noaniqligi xalqaro xavfsizlik tizimini sezilarli darajada o‘zgartirmoqda. Bu jarayon bir nechta asosiy yo‘nalishlarda namoyon bo‘ladi. Avvalo, xavfsizlik dilemmasi va ishonchsizlik kuchaymoqda: kiberhujumni aniq aniqlashning qiyinligi davlatlar o‘rtasida shubha va ehtiyotkorlikni oshiradi, natijada bir tomonning mudofaa harakati boshqasi tomonidan agressiya sifatida qabul qilinishi mumkin. Shuningdek, nazoratsiz kiber qurollanish poygasi kuchayib bormoqda. Davlatlar kiber salohiyatini tez sur’atda rivojlantirmoqda, biroq bu sohada xalqaro nazorat mexanizmlarining yetarli emasligi vaziyatni yanada beqarorlashtiradi. Bundan tashqari, gibrid urushlar va infratuzilmalarning zaifligi muhim xavf sifatida yuzaga chiqmoqda. Kiberhujumlar endi faqat raqamli tizimlarga emas, balki energetika, moliya va sog‘liqni saqlash kabi hayotiy infratuzilmalarga ham bevosita ta’sir ko‘rsatib, urushsiz strategik zarba berish imkonini yaratmoqda.WannaCry (2017) ransomware hujumi 150 dan ortiq davlatda 200 mingdan ziyod kompyuterni zararladi. U fayllarni shifrlab, to‘lov talab qilgan va ayniqsa Buyuk Britaniya NHS tizimida kasalxonalar ishini vaqtincha to‘xtatgan. Bu hodisa kiberhujumlar muhim infratuzilmalarni jiddiy izdan chiqarishi mumkinligini ko‘rsatadi.[37]

Xalqaro munosabatlar va xalqaro huquq nuqtai nazaridan kibermakon bugungi kunda tobora geosiyosiy raqobat maydoniga aylanib bormoqda. Biroq ushbu sohani tartibga soluvchi mavjud huquqiy mexanizmlar asosan an’anaviy, hududiy chegaralarga asoslangan xalqaro tizim doirasida shakllangan bo‘lib, kibermakonning o‘ziga xos xususiyatlariga to‘liq mos kelmaydi. Shu sababli global kiberboshqaruvda sezilarli huquqiy bo‘shliqlar saqlanib qolmoqda. Avvalo, hozirgi xalqaro kelishuvlarning kiberfazoda to‘liq ishlamasligining asosiy sababi atributsiya muammosi bilan bog‘liq. Ya’ni kiberhujumlarni amalga oshirgan aniq subyektni ishonchli tarzda aniqlash deyarli har doim murakkab bo‘lib qoladi. Bu esa davlatlarga javobgarlikdan qochish yoki noaniqlikni siyosiy vosita sifatida ishlatish imkonini beradi. Bundan tashqari, xalqaro huquqda “kuch ishlatish” tushunchasi an’anaviy ravishda jismoniy harbiy vositalar bilan bog‘liq holda talqin qilinadi. Kiberhujumlar esa ba’zan jiddiy iqtisodiy yoki infratuzilmaviy zarar yetkazsada, ularning qurolli hujum

[37]https://www.cloudflare.com/ru-ru/learning/security/ransomware/wannacry-ransomware/

sifatidagi huquqiy maqomi bo‘yicha yagona xalqaro konsensus mavjud emas. Shu bilan birga, texnologik rivojlanish tezligi va xalqaro huquqni ishlab chiqish jarayonining sekinligi o‘rtasidagi nomutanosiblik ham ushbu muammoni yanada chuqurlashtirmoqda. Mazkur sharoitda Tallinn Manual kiberhuquq sohasidagi eng muhim akademik tashabbuslardan biri sifatida e’tirof etiladi. Ushbu hujjat kibermakonda xalqaro huquq normalarini qo‘llash imkoniyatlarini tizimli tarzda tahlil qilib, davlat suvereniteti, ehtiyotkorlik prinsipi hamda kiberoperatsiyalar jarayonida inson huquqlarini himoya qilish kabi masalalarni yoritadi.[38]Shu bilan birga, u kiberfazoni huquqiy bo‘shliq emas, balki amaldagi xalqaro huquq tatbiq etilishi mumkin bo‘lgan makon sifatida talqin qiladi. Biroq uning asosiy cheklovi shundaki, u majburiy xalqaro shartnoma emas, balki ekspertlar tomonidan ishlab chiqilgan tavsiyaviy hujjat hisoblanadi. Bundan tashqari, uning yondashuvi asosan G‘arb davlatlari pozitsiyasini aks ettiradi va ayrim davlatlar, jumladan Rossiya hamda Xitoy tomonidan to‘liq qabul qilinmagan. Bu holat kiberboshqaruv sohasida global konsensus shakllanishini yanada murakkablashtiradi.

Olib borilgan tahlillar shuni ko‘rsatadiki, kibermakonning globallashuvi xalqaro xavfsizlik tizimini murakkablashtirib, mavjud huquqiy va institutsional mexanizmlarning yetarli emasligini yaqqol namoyon etmoqda. Atributsiya muammosi, kiberhujumlarning transchegaraviy tabiati hamda yagona global boshqaruv modelining yo‘qligi davlatlar o‘rtasida ishonchsizlikni kuchaytirib, xavfsizlik muvozanatini zaiflashtirmoqda. Shu nuqtayi nazardan, xalqaro xavfsizlikni ta’minlash uchun yangi yondashuvlar va amaliy mexanizmlarni ishlab chiqish zarur. Birinchi navbatda, davlatlar o‘rtasida ishonchni mustahkamlovchi choralarni kuchaytirish muhim ahamiyatga ega. Bunga kiberhodisalar bo‘yicha tezkor axborot almashinuvi, shaffoflikni oshirish, milliy kiber strategiyalar haqida muntazam muloqot va krizis holatlarida aloqa kanallarini yo‘lga qo‘yish kiradi. Bunday mexanizmlar noto‘g‘ri talqin qilinadigan kiberoperatsiyalar va keskinlashuv xavfini kamaytirishga xizmat qiladi. Ikkinchidan, kibermakonni tartibga solish bo‘yicha kiber-qurollarni nazorat qiluvchi yangi xalqaro konvensiyalarni ishlab chiqish zarur. Amaldagi huquqiy asoslar yetarli darajada aniq emasligi sababli, kiberqurollarning ta’rifi, ulardan foydalanish chegaralari hamda javobgarlik mexanizmlarini belgilovchi umumiy xalqaro kelishuvlar ishlab chiqilishi lozim. Bu esa kibermakonda strategik barqarorlikni ta’minlashga va kiberqurollanish poygasini cheklashga xizmat qiladi.

Xulosa

Zamonaviy xalqaro xavfsizlik tizimi tobora murakkablashib, an’anaviy harbiy kuchlar muvozanatidan tashqari yangi – raqamli o‘lchovga ham tayanmoqda. Kibermakonning global siyosiy, iqtisodiy va texnologik jarayonlardagi o‘sib borayotgan roli davlatlar o‘rtasidagi kuchlar muvozanatini qayta shakllantirmoqda. Bu esa nafaqat texnik, balki chuqur siyosiy va huquqiy muammolarni ham yuzaga keltiradi. Xususan, kiberhujumlar, atributsiya muammosi va asimmetrik imkoniyatlar xalqaro xavfsizlik barqarorligiga bevosita ta’sir ko‘rsatadi. Shu nuqtayi nazardan, kelajakda “kiber-tinchlik” konsepsiyasini rivojlantirish dolzarb ahamiyat kasb etadi. Mazkur yondashuv orqali davlatlarning kiber salohiyatidan faqat mudofaa, infratuzilmalarni himoya qilish va barqaror rivojlanish

[38] “Tallinn Manual on the international law applicable to cyber warfare” Michael N.Schmitt

maqsadlarida foydalanilishi ta'minlanishi mumkin. Buning uchun global konsensusga erishish, umumiy kiber-etika normalarini shakllantirish va xalqaro hamkorlikni yangi bosqichga olib chiqish zarur. Kibermakonda ishonchni mustahkamlovchi mexanizmlar va huquqiy asoslarning yaratilishi raqamli mojarolar xavfini kamaytiradi. Natijada, texnologik taraqqiyot keltirib chiqarayotgan tahdidlarni jilovlash hamda global xavfsizlikni yangi raqamli davr sharoitida saqlab qolish imkoniyati sezilarli darajada kengayadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. "Cyber Power" by Joseph Nye
2. https://researchcorridor.org/index.php/ijcnw/article/view/521
3. "The future of power" by Joseph Nye
4. https://www.nature.com/articles/s41599-025-04897-7
5. https://www.sciencedirect.com/science/article/abs/pii/S187454821400002X
6. https://www.hypr.com/security-encyclopedia/notpetya
7. https://www.cloudflare.com/ru-ru/learning/security/ransomware/wannacry-ransomware/
8. "Tallinn Manual on the international law applicable to cyber warfare" Michael N.Schmitt