GIBRID MOJAROLAR SHAROITIDA AXBOROT XAVFSIZLIGINI TA'MINLASHDA DAVLATLARARO HAMKORLIKNING SIYOSIY MEXANIZMLARI

Yasinbek Xazratqulov Baxtiyorjon o'g'li
Email: yasinhazratqulov823@gmail.com
ORCID ID: https://orcid.org/0009-0001-4658-9477

Annotatsiya: Maqolada gibrid mojarolar sharoitida axborot xavfsizligini ta'minlashda davlatlararo hamkorlikning siyosiy mexanizmlari tahlil qilinadi. Axborot tahdidlarining transchegaraviy xususiyati, hamkorlikning global, mintaqaviy va ikki tomonlama darajalari hamda xalqaro yondashuvlar qiyosiy o'rganiladi. Markaziy Osiyo va O'zbekiston uchun mintaqaviy hamkorlikni rivojlantirish bo'yicha takliflar ishlab chiqilgan.

Kalit so'zlar: gibrid mojaro, axborot xavfsizligi, kiberxavfsizlik, dezinformatsiya, davlatlararo hamkorlik.

XXI asrda xalqaro munosabatlar tizimida xavfsizlikka tahdidlarning mazmuni va namoyon bo'lish shakllari sezilarli darajada o'zgarib bormoqda. Zamonaviy mojarolarda an'anaviy harbiy vositalar bilan bir qatorda siyosiy, iqtisodiy, axborot va kiber vositalarning o'zaro uyg'unlashuvi kuzatilmoqda. Mazkur jarayon xalqaro xavfsizlik tadqiqotlarida "gibrid mojarolar" va "gibrid tahdidlar" tushunchalarining dolzarblashuviga olib kelmoqda. Bunday tahdidlar davlatning siyosiy institutlari, ijtimoiy barqarorligi, jamoatchilik fikri va strategik infratuzilmasiga bevosita yoki bilvosita ta'sir ko'rsatishi mumkin.

Gibrid tahdidlarning muhim tarkibiy qismlaridan biri axborot makonidan siyosiy maqsadlarda foydalanish bilan bog'liq. Dezinformatsiya va manipulyativ axborot kampaniyalari, ijtimoiy tarmoqlar orqali jamoatchilik fikriga ta'sir ko'rsatish, axborot-kommunikatsiya infratuzilmasiga kiberhujumlar hamda davlatlarning siyosiy jarayonlariga tashqi axborot ta'siri xalqaro xavfsizlikning yangi muammolari sifatida namoyon bo'lmoqda. BMT doirasida ham axborot-kommunikatsiya texnologiyalaridan foydalanishning xalqaro xavfsizlikka ta'siri, davlatlarning mas'uliyatli xatti-harakatlari, xalqaro huquq normalari va davlatlararo hamkorlik masalalari izchil muhokama qilinmoqda.

Mazkur tahdidlarning o'ziga xos jihatlaridan biri ularning transchegaraviy xarakterga egaligidir. Raqamli va axborot makonidagi tahdidlar davlat hududi bilan cheklanib qolmay, qisqa vaqt ichida boshqa davlatlar va butun mintaqa axborot makoniga ta'sir ko'rsatishi mumkin. Shu bois axborot xavfsizligini ta'minlash masalasi faqat milliy siyosat doirasida emas, balki xalqaro va

mintaqaviy hamkorlikning muhim yo‘nalishi sifatida qaralishi lozim.

Xalqaro amaliyotda mazkur yo‘nalishdagi davlatlararo hamkorlikning muhim misollaridan biri Shanxay Hamkorlik Tashkiloti doirasida 2009-yil 16-iyunda imzolangan “Xalqaro axborot xavfsizligini ta’minlash sohasida hamkorlik to‘g‘risida”gi [1] bitimdir. Mazkur hujjat ShHTga a’zo davlatlar o‘rtasida xalqaro axborot xavfsizligini ta’minlash bo‘yicha hamkorlikning huquqiy va tashkiliy asoslarini belgilaydi hamda tahdidlarni monitoring qilish, ularga javob choralarini muvofiqlashtirish va hamkorlik mexanizmlarini rivojlantirish masalalarini qamrab oladi.

O‘zbekiston uchun ham mazkur masala alohida ahamiyat kasb etadi. Xususan, 2022-yil 15-aprelda qabul qilingan O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi [2] Qonun kiberxavfsizlik sohasidagi munosabatlarni huquqiy jihatdan tartibga solib, shaxs, jamiyat va davlat manfaatlarini kibermakondagi tashqi va ichki tahdidlardan himoya qilishga qaratilgan. Qonunda O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi ham asosiy prinsiplardan biri sifatida belgilangan.

Shu bilan birga, Markaziy Osiyoda axborot va kiberxavfsizlik masalalarini faqat milliy xavfsizlik nuqtayi nazaridan emas, balki davlatlararo siyosiy munosabatlar, mintaqaviy xavfsizlik va xalqaro hamkorlik kontekstida tizimli tadqiq etish zarurati saqlanib qolmoqda. Ayniqsa, tahdidlar to‘g‘risida axborot almashinuvi, o‘zaro ishonchni mustahkamlash, umumiy yondashuvlarni shakllantirish, davlatlararo muloqot va hamkorlik mexanizmlarini rivojlantirish masalalari ilmiy tahlilni talab etadi. BMTning xalqaro xavfsizlik kontekstidagi ICT masalalariga bag‘ishlangan muzokaralarida ham tahdidlarni aniqlash, hamkorlik choralarini ishlab chiqish, xalqaro huquqni qo‘llash va davlatlar o‘rtasida ishonchni mustahkamlash masalalariga alohida e’tibor qaratilgan. Mazkur tadqiqotning dolzarbligi shundan iboratki, gibrid mojarolar sharoitida axborot xavfsizligini ta’minlashning davlatlararo siyosiy mexanizmlarini, ularning xalqaro va mintaqaviy darajadagi institutsional asoslarini hamda samaradorlik omillarini tizimli o‘rganish, Markaziy Osiyo davlatlari tajribasini qiyosiy tahlil qilish va O‘zbekistonning mintaqaviy hamkorlik siyosatini takomillashtirishga qaratilgan ilmiy-amaliy takliflarni ishlab chiqish zarurati mavjuddir.

Gibrid mojarolar sharoitida axborot omilining o‘rni. Zamonaviy xalqaro munosabatlar tizimida gibrid mojarolar davlatlar o‘rtasidagi qarama-qarshilikning murakkab shakli sifatida namoyon bo‘lib, ularda harbiy vositalar bilan bir qatorda siyosiy, iqtisodiy, axborot va kiber vositalardan kompleks foydalanish kuzatiladi [3]. Mazkur yondashuv gibrid mojaro tushunchasining nafaqat harbiy qarama-qarshilik, balki davlatlararo siyosiy raqobat va xalqaro xavfsizlik nuqtayi nazaridan ham tadqiq etilishini taqozo

etadi. Gibrid mojarolarda axborot omili alohida strategik ahamiyatga ega. Dezinformatsiya, manipulyativ axborot kampaniyalari, jamoatchilik fikriga ta'sir ko'rsatish, raqamli kommunikatsiya kanallaridan siyosiy maqsadlarda foydalanish hamda axborot-kommunikatsiya infratuzilmasiga kiberhujumlar davlatlarning siyosiy barqarorligi va milliy manfaatlariga ta'sir ko'rsatishi mumkin [4]. Shu jihatdan axborot omili zamonaviy xalqaro raqobatning muhim vositasi sifatida namoyon bo'ladi.

Mazkur tadqiqot doirasida gibrid mojarolardagi axborot tahdidlarini uch guruhga ajratish mumkin:

– **texnologik tahdidlar** – axborot-kommunikatsiya tizimlari va muhim infratuzilmaga qarshi kiberhujumlar;

– **kognitiv-axborot tahdidlar** – dezinformatsiya, manipulyativ kontent va jamoatchilik fikriga maqsadli ta'sir ko'rsatish;

– **institutsional-siyosiy tahdidlar** – davlat institutlari, siyosiy jarayonlar va davlat boshqaruviga nisbatan ishonchni zaiflashtirishga qaratilgan ta'sirlar [5].

Ushbu tasnif muallifning tahliliy yondashuvi sifatida tahdidlarning texnik xususiyatlari bilan bir qatorda ularning siyosiy va institutsional oqibatlarini ham hisobga olish imkonini beradi. Axborot tahdidlarining transchegaraviy xususiyati ularni faqat milliy xavfsizlik doirasida hal etish imkoniyatlarini cheklaydi. Kiberhujumlar, raqamli dezinformatsiya va transmilliy axborot kampaniyalari turli davlatlar hududidan amalga oshirilishi mumkinligi sababli ularning manbasini aniqlash, atributsiya qilish va ularga javob berish davlatlararo hamkorlikni talab qiladi [6]. Shu sababli axborot xavfsizligi zamonaviy xalqaro munosabatlarda nafaqat milliy, balki mintaqaviy va global xavfsizlik masalasi sifatida ham qaralmoqda.

Davlatlararo hamkorlik mexanizmlarining asosiy darajalari. Axborot xavfsizligini ta'minlash sohasidagi davlatlararo hamkorlikni global, mintaqaviy va ikki tomonlama darajalarda tahlil qilish mumkin. **Global darajada** BMT doirasida axborot-kommunikatsiya texnologiyalaridan xalqaro xavfsizlikka zarar yetkazmaydigan va mas'uliyatli tarzda foydalanish masalalari muhokama qilinib kelmoqda. Hukumat ekspertlari guruhlari (GGE) va Ochiq tarkibli ishchi guruhlar (OEWG) faoliyati natijasida davlatlarning mas'uliyatli xatti-harakatlari, xalqaro huquqning qo'llanilishi, davlatlararo hamkorlik va ishonchni mustahkamlashga qaratilgan yondashuvlar shakllangan [7].

Xalqaro huquqning kiberfazoga tatbiq etilishi masalalarini tahlil qiluvchi **Tallinn Manual** ham ushbu yo'nalishdagi muhim ekspert manbalaridan biri hisoblanadi. Biroq u xalqaro shartnoma yoki majburiy huquqiy hujjat emas, balki xalqaro huquq ekspertlari tomonidan ishlab chiqilgan tahliliy qo'llanmadir [8]. **Mintaqaviy darajada** turli xalqaro tashkilotlar doirasida

axborot va kiberxavfsizlik bo‘yicha hamkorlik mexanizmlari shakllangan. Xususan, Shanxay Hamkorlik Tashkiloti doirasida 2009-yilda **“Xalqaro axborot xavfsizligini ta’minlash sohasida hamkorlik to‘g‘risida”gi bitim**ning imzolanishi a’zo davlatlarning mazkur yo‘nalishdagi hamkorligini institutsional jihatdan mustahkamlashga qaratilgan muhim qadam bo‘ldi [9].

Yevropa hududida esa Yevropa Ittifoqi va NATO doirasida gibrid tahdidlarga qarshi chidamlilikni oshirish, kiberxavfsizlik, strategik kommunikatsiya va davlatlararo hamkorlikni kuchaytirishga qaratilgan mexanizmlar shakllangan. 2017-yilda tashkil etilgan **Yevropa Gibrid Tahdidlarga qarshi kurashish mukammallik markazi (Hybrid CoE)** mazkur yo‘nalishdagi hamkorlik va ekspertlar almashinuvining muhim platformalaridan biridir [10]. **Ikki tomonlama darajada** esa davlatlar o‘rtasidagi axborot almashinuvi, kiberhodisalarga javob berish, vakolatli organlar o‘rtasidagi muloqot va texnik ekspertlar almashinuvi muhim ahamiyat kasb etadi. Bunday mexanizmlar tahdidlarga tezkor javob berish bilan birga, davlatlar o‘rtasidagi o‘zaro ishonchni mustahkamlashga xizmat qiladi.

Xalqaro yondashuvlarning qiyosiy tahlili. Tadqiqot shuni ko‘rsatadiki, xalqaro maydonda axborot va kiberxavfsizlik masalalariga nisbatan yondashuvlar institutsional va normativ jihatdan bir xil emas. Ayrim davlatlar axborot makonida davlat suvereniteti, davlatlarning ichki ishlariga aralashmaslik va axborot xavfsizligini ta’minlashga katta e’tibor qaratsa, boshqa davlatlar ochiq, barqaror va xavfsiz raqamli makonni rivojlantirish, inson huquqlari hamda xalqaro huquq normalarini qo‘llash masalalarini ustuvor deb hisoblaydi [11]. Shu sababli ushbu yondashuvlarni qat’iy qarama-qarshi bloklar sifatida emas, balki xalqaro axborot xavfsizligining turli siyosiy-normativ talqinlari sifatida baholash maqsadga muvofiq.

Markaziy Osiyo va O‘zbekiston uchun muammolar. Markaziy Osiyo davlatlari uchun axborot xavfsizligi masalasi raqamli transformatsiya, davlat xizmatlarining elektronlashuvi va axborot-kommunikatsiya texnologiyalarining kengayishi sharoitida tobora muhimlashib bormoqda. Shu bilan birga, mintaqadagi davlatlarning axborot xavfsizligi siyosati va institutsional imkoniyatlari o‘rtasida muayyan farqlar mavjud.

O‘zbekistonda 2022-yil 15-aprelda qabul qilingan **O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonun** kiberxavfsizlik sohasidagi munosabatlarni huquqiy jihatdan tartibga solishning muhim asosini yaratdi [12]. Mazkur qonunda kiberxavfsizlikni ta’minlash, muhim axborot infratuzilmasini himoya qilish va xalqaro hamkorlik masalalariga e’tibor qaratilgan. Shu bilan birga, Markaziy Osiyo miqyosida axborot tahdidlarini monitoring qilish, vakolatli organlar o‘rtasida tezkor axborot almashinuvi, kiberhodisalarga javob berish va dezinformatsiyaga qarshi hamkorlik bo‘yicha mintaqaviy

mexanizmlarni yanada rivojlantirish zarur. Ayniqsa, davlatlar o‘rtasidagi siyosiy ishonch, milliy manfaatlar va axborot suverenitetiga oid turli yondashuvlar bunday hamkorlikni shakllantirishda hisobga olinishi lozim.

Xulosa qilganda, tadqiqot natijalari shuni ko‘rsatadiki, gibrid mojarolar sharoitida axborot xavfsizligi davlatlarning milliy xavfsizligi bilan bir qatorda xalqaro va mintaqaviy xavfsizlikning muhim tarkibiy qismiga aylanmoqda. Axborot va kiber tahdidlarning transchegaraviy xususiyati ularni faqat milliy darajada bartaraf etish imkoniyatlarini cheklab, davlatlararo hamkorlikni kuchaytirishni talab etadi. Shu nuqtayi nazardan, Markaziy Osiyo davlatlari o‘rtasida axborot tahdidlariga oid ma’lumot almashish, kiberhodisalarga tezkor javob berish va siyosiy maslahatlashuvlarning doimiy mexanizmlarini rivojlantirish maqsadga muvofiq. Shuningdek, xalqaro tashkilotlar doirasidagi hamkorlikni faollashtirish, mintaqaviy ekspert-tahlil tarmoqlarini shakllantirish hamda aholining axborot savodxonligini oshirish mintaqaning axborot barqarorligini mustahkamlashga xizmat qiladi. Umuman, axborot xavfsizligini ta’minlash texnik choralar bilan cheklanmasdan, davlatlararo siyosiy hamkorlik, mintaqaviy xavfsizlik va xalqaro huquq tamoyillari asosida kompleks yondashuvni talab etadi.

FOYDALANILGAN ADABIYOTLAR

1. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности: заключено в г. Екатеринбурге 16 июня 2009 г. Url: https://rus.sectsco.org/20090616/203974.html
2. O‘zbekiston Respublikasining Qonuni. Kiberxavfsizlik to‘g‘risida: 2022-yil 15-apreldagi O‘RQ-764-son // Qonunchilik ma’lumotlari milliy bazasi. Url: https://lex.uz/uz/docs/-5960604
3. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. – Arlington: Potomac Institute for Policy Studies, 2007.
4. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making: Council of Europe Report DGI(2017)09. – Strasbourg: Council of Europe, 2017.
5. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. – New York: Farrar, Straus and Giroux, 2020.
6. Rid T., Buchanan B. Attributing Cyber Attacks // Journal of Strategic Studies, 2015. Vol. 38, № 1–2. – P. 4–37.
7. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: UN

Doc. A/76/135, New York: United Nations, 2021.
8. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt, 2nd ed. Cambridge: Cambridge University Press, 2017.
9. The European Centre of Excellence for Countering Hybrid Threats: official website, Helsinki. Url: https://www.hybridcoe.fi
10. Nocetti J. Contest and conquest: Russia and global internet governance // International Affairs, 2015. Vol. 91, № 1. – P. 111-130.