KIBERJINOYATCHILIK VA XALQARO HUQUQ: TRANSCHEGARAVIY KIBERHUJUMLARDA DAVLATLARNING JAVOBGARLIGI MASALASI

Xushboqov Umidbek
TerDU, Yurisprudensiya ta’lim yo’nalishi 2-bosqich talabasi

Annotatsiya: *Raqamli texnologiyalar rivoji bilan transchegaraviy kiberhujumlar global xavfsizlikka jiddiy tahdidga aylandi. Ushbu maqolada kiberjinoyatchilikning xalqaro huquqiy jihatlari, xususan, transchegaraviy kiberhujumlarda davlatlarning javobgarligi masalasi ko‘rib chiqiladi. O‘zbekiston Respublikasining milliy qonunchiligi va xalqaro huquq normalari solishtirilgan holda tahlil qilinadi. Tadqiqot natijasida atributsiya muammosi, davlatning tegishli ehtiyot choralarini ko‘rish (due diligence) majburiyati va xalqaro hamkorlikning dolzarbligi ko‘rsatiladi. Maqola O‘zbekiston qonunchiligini takomillashtirish bo‘yicha amaliy tavsiyalarni ham o‘z ichiga oladi.*

Kalit so‘zlar: *kiberjinoyatchilik, transchegaraviy kiberhujum, davlat javobgarligi, xalqaro huquq, atributsiya, due diligence, O‘zbekiston Jinoyat kodeksi, Tallinn Manual.*

Bugungi kunda kibermakon butun dunyo uchun ham imkoniyatlar, ham xavflar manbaiga aylangan. Internet va raqamli texnologiyalar rivoji bilan birga kiberjinoyatchilik ham keskin kuchaydi. Ayniqsa, transchegaraviy kiberhujumlar, ya’ni bir davlat hududidan ikkinchi davlatga qaratilgan hujumlar katta iqtisodiy zarar yetkazishi, muhim infratuzilmani ishdan chiqarishi va hatto milliy xavfsizlikka tahdid solishi mumkin.

Bunday hujumlarning o‘ziga xos jihati shundaki, ularni sodir etgan shaxslarning shaxsini aniqlash va ularni javobgarlikka tortish juda qiyin. Jinoyatchilar proxy serverlar, botnetlar va boshqa texnik vositalardan foydalanib, o‘z izlarini yashirishadi. Shu bois savol tug‘iladi, agar kiberhujum davlat organlari yoki ularning nazoratidagi shaxslar tomonidan amalga oshirilsa, bu holatda qaysi davlat xalqaro huquq oldida javobgar bo‘ladi?

Ushbu maqolaning asosiy maqsadi, transchegaraviy kiberhujumlarda davlatlarning javobgarligi masalasini O‘zbekiston milliy qonunchiligi va xalqaro huquq normalari asosida tahlil qilishdir. Tadqiqotda milliy va xalqaro huquqiy hujjatlar qiyosiy tahlil qilinadi hamda O‘zbekiston uchun amaliy tavsiyalar ishlab chiqiladi.

Kiberjinoyatchilik va davlat javobgarligi masalasi xalqaro huquqshunoslikda faol muhokama qilinmoqda. Bu borada eng muhim manbalardan biri Tallinn Manual 2.0 hisoblanadi. Ushbu qo‘llanma NATO ekspertlari tomonidan tayyorlangan bo‘lib, kibermakonda xalqaro huquq normalarini qo‘llash masalalarini chuqur yoritadi. Unda davlatning suvereniteti, javobgarligi va tegishli ehtiyot choralarini ko‘rish majburiyati kabi masalalar batafsil ko‘rib chiqilgan.

Xalqaro darajada yana bir asosiy hujjat Kiberjinoyatlar to‘g‘risidagi Budapesht Konvensiyasi (2001-yil). Bu konvensiya kiberjinoyatlarni milliy qonunlarda jinoiy

javobgarlikka tortish va xalqaro hamkorlikni kuchaytirishga qaratilgan birinchi ko‘p tomonlama shartnoma hisoblanadi. O‘zbekiston hozircha ushbu Konvensiyaga qo‘shilmagan, ammo MDH davlatlari o‘rtasidagi axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurash bo‘yicha Bitimni ratifikatsiya qilgan. Shuningdek, O‘zbekiston BMTning yangi Kiberjinoyatchilikka qarshi Konvensiyasini imzolagan.

O‘zbekiston milliy qonunchiligida kiberjinoyatlar Jinoyat kodeksining XX-1 bobi (“Axborot texnologiyalari sohasidagi jinoyatlar”) bilan tartibga solinadi. Bu bobda quyidagi moddalar mavjud: 278²-modda – kompyuter axborotidan qonunga xilof ravishda foydalanish; 278⁴-modda – kompyuter axborotini modifikatsiyalashtirish; 278⁵-modda – kompyuter sabotaji; 278⁶-modda – zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish va boshqalar.

2024-yilda Jinoyat kodeksiga kripto-aktivlar bilan bog‘liq yangi moddalar (278⁸ va 278⁹-moddalar) qo‘shilgan. Bundan tashqari, 2022-yilda qabul qilingan “Kiberxavfsizlik to‘g‘risida”gi Qonun (O‘RQ-764-son) kiberxavfsizlikni ta’minlashning asosiy prinsiplarini, davlat organlarining vakolatlarini va xalqaro hamkorlikni mustahkamlaydi. Qonunga ko‘ra, vakolatli organ sifatida Davlat xavfsizlik xizmati (DXX) belgilangan.

Tadqiqotda qiyosiy-huquqiy, tizimli-tahliliy va formaldogmatik usullar qo‘llanildi. Lex.uz milliy qonunchilik bazasi, xalqaro shartnomalar va ilmiy adabiyotlar tahlil qilindi.

O‘zbekiston milliy qonunchiligi ichki kiberjinoyatlarga qarshi kurashda yetarli huquqiy asos yaratgan. Jinoyat kodeksida axborot texnologiyalari sohasidagi jinoyatlar uchun aniq jazo choralarini ko‘zda tutuvchi moddalar mavjud. Masalan, kompyuter tizimini qasddan ishdan chiqarish (kompyuter sabotaji) uchun jarima yoki ozodlikdan mahrum qilish jazosi belgilangan. “Kiberxavfsizlik to‘g‘risida”gi Qonun esa kiberxavfsizlik hodisalarini tekshirish, muhim axborot infratuzilmasini himoya qilish va xalqaro hamkorlikni rivojlantirish masalalarini tartibga soladi.

Biroq transchegaraviy kiberhujumlar masalasida milliy qonunlar yetarli emas. Hujumni boshqa davlat hududidan sodir etilgan taqdirda jinoyatchini aniqlash, dalillarni yig‘ish va uni javobgarlikka tortishda katta texnik va huquqiy qiyinchiliklar yuzaga keladi.

Xalqaro huquqda davlat javobgarligi asosan Davlat javobgarligi to‘g‘risidagi moddalar (Xalqaro huquq komissiyasi, 2001) ga asoslanadi. Davlat javobgarligi ikki asosiy shart bilan yuzaga keladi: harakat (yoki harakatsizlik) davlatga bog‘lanishi (atributsiya) va xalqaro majburiyatning buzilishi.

Tallinn Manual 2.0 ga ko‘ra, davlat o‘z organlari tomonidan sodir etilgan kiberoperatsiyalar uchun to‘g‘ridan-to‘g‘ri javobgar bo‘ladi. Agar hujum davlat nazoratidagi nodavlat shaxslar tomonidan amalga oshirilsa ham, davlatning ko‘rsatmasi yoki nazorati mavjud bo‘lsa, bu harakat davlatga tegishli hisoblanadi. Bundan tashqari, har qanday davlat o‘z hududidan boshqa davlatlarga qarshi kiberhujumlar sodir etilishiga yo‘l qo‘ymaslik uchun due diligence (tegishli ehtiyot choralarini ko‘rish) majburiyatini bajarishi

shart. Agar davlat hujum haqida bilgan bo‘lsa va uni oldini olish uchun yetarli choralar ko‘rmagan bo‘lsa, u xalqaro huquq oldida javobgarlikka tortilishi mumkin.

Eng katta muammo atributsiya, ya’ni hujumni aniq bir davlatga bog‘lash. Texnik jihatdan bu jarayon murakkab bo‘lib, ko‘pincha ishonchli dalillar yetishmaydi.

O‘zbekiston qonunchiligi ichki kiberjinoyatlarni jazolashda yaxshi asosga ega bo‘lsa-da, transchegaraviy kontekstda yetarli emas. Milliy qonunlarda davlatning o‘z hududidan chiqib ketadigan kiberhujumlarga nisbatan due diligence majburiyati aniq belgilab qo‘yilmagan. Xalqaro tajribada esa, hatto jismoniy zarar bo‘lmagan taqdirda ham muhim infratuzilmani vaqtincha ishdan chiqarish suverenitetni buzish sifatida baholanishi mumkin.

Hozirgi vaqtda atributsiya yetishmovchiligi, xalqaro hamkorlik mexanizmlarining cheklanganligi va raqamli dalillarni tan olish masalalari dolzarb muammolar hisoblanadi. O‘zbekiston Budapesht Konvensiyasiga qo‘shilmagan bo‘lsa-da, MDH Bitimi va yangi BMT Konvensiyasi doirasida hamkorlikni rivojlantirmoqda. Bu yo‘nalishda yanada faolroq harakat qilish zarur.

“Raqamli O‘zbekiston – 2030” strategiyasi doirasida muhim axborot infratuzilmasini himoya qilish masalasi alohida ahamiyatga ega. Shuning uchun milliy qonunchilikni xalqaro standartlarga yaqinlashtirish va xalqaro hamkorlikni kuchaytirish lozim.

Xulosa qilib aytganda, Transchegaraviy kiberhujumlarda davlatlarning javobgarligi xalqaro huquqning rivojlanayotgan va murakkab sohasidir. O‘zbekiston milliy qonunchiligi ichki tahdidlarga qarshi kurashda muayyan asos yaratgan, ammo xalqaro miqyosda atributsiya va due diligence mexanizmlarini mustahkamlash talab etiladi. Global hamkorliksiz bu tahdidlarni samarali bartaraf etish qiyin. O‘zbekiston “Kiberxavfsizlik to‘g‘risida”gi Qonunda belgilangan xalqaro hamkorlik prinsipini amalda kuchaytirishi, Budapesht Konvensiyasiga qo‘shilish masalasini ko‘rib chiqishi va raqamli dalillar bilan ishlash tartibini takomillashtirishi lozim. Bu nafaqat milliy xavfsizlikni, balki raqamli iqtisodiyotning barqaror rivojlanishini ham ta’minlaydi.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasi Jinoyat kodeksi (lex.uz).
2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni (O‘RQ-764-son, 2022-yil).
3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.
4. Budapest Convention on Cybercrime (2001).
5. MDH davlatlari o‘rtasidagi axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurash bo‘yicha Bitim (2018).
6. Schmitt M.N. va boshq. Tallinn Manual 2.0 sharhlari.
7. Lex.uz rasmiy ma’lumotlar bazasi va boshqa ilmiy manbalar.