

**KIBERHUJUMLAR UCHUN DAVLATLARNING XALQARO-HUQUQIY
JAVOBGARLIGI**

Jo'rayev Javoxir Meliboy o'g'li

Toshkent davlat yuridik universiteti tyutori

Toshkent, O'zbekiston

jjuraev571@gmail.com

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi zamonaviy jamiyat hayotining barcha sohalarini qamrab olgan bo'lib, ayni paytda davlatlar xavfsizligiga qaratilgan yangi tahdid - kiberhujumlarning kuchayishiga sabab bo'lmoqda. Kritik infratuzilma obyektlariga, davlat axborot tizimlariga va moliyaviy sohaga yo'naltirilgan kiberhujumlar milliy xavfsizlik, iqtisodiy barqarorlik va xalqaro tinchlik uchun jiddiy xatar tug'dirmoqda. Shu bois davlatlarning bunday hujumlar uchun xalqaro-huquqiy javobgarligi masalasi zamonaviy xalqaro huquqning eng dolzarb muammolaridan biriga aylandi.

Xalqaro huquqda davlatning javobgarligi uning xalqaro-huquqiy majburiyatini buzuvchi xatti-harakati (yoki harakatsizligi) sodir etilishi bilan yuzaga keladi. BMTning Xalqaro huquq komissiyasi tomonidan ishlab chiqilgan "Davlatlarning xalqaro nomaqbul xatti-harakatlar uchun javobgarligi to'g'risidagi moddalar" [1] ushbu institutning asosiy me'yoriy negizini tashkil etadi. Kiberhujumlar kontekstida bu qoidalar to'liq qo'llaniladi: agar hujum davlatga tegishli deb topilsa va u davlatning xalqaro majburiyatini buzsa, davlat javobgarlikka tortilishi mumkin.

Kiberhujumlarga nisbatan amaldagi xalqaro huquq normalarining qo'llanilishi masalasi maxsus e'tiborni talab qiladi. BMT hukumat ekspertlari guruhi (UN GGE) o'z hisobotlarida amaldagi xalqaro huquq, jumladan BMT Nizomi [2], kiberfazoga ham tatbiq etilishini tasdiqlagan. Davlat suvereniteti, kuch ishlatishni taqiqlash va boshqa davlatning ichki ishlariga aralashmaslik tamoyillari kibersohada ham amal qiladi. Kiberhujumlarga xalqaro huquqning qo'llanilishini

batafsil sharhlovchi “Tallinn qo‘llanmasi 2.0” [3] esa nufuzli doktrinal manba sifatida e’tirof etilgan.

Davlat javobgarligini belgilashda eng murakkab masala - hujumni muayyan davlatga bog‘lash (atributsiya) muammosidir. Kiberhujumlarning texnik xususiyatlari, ya’ni manbani yashirish, uchinchi davlatlar serverlaridan foydalanish va harakatlarni anonim tarzda amalga oshirish imkoniyati hujum ijrochisini aniqlashni jiddiy qiyinlashtiradi. Xalqaro huquqda hujum davlatga u davlatning organlari tomonidan sodir etilganda yoxud davlat nazorati ostidagi shaxslar tomonidan amalga oshirilganda bog‘lanadi. Biroq kiberfazoda zarur nazorat darajasini isbotlash ko‘pincha texnik va huquqiy jihatdan o‘ta murakkab bo‘lib qoladi.

Amaliyotda davlatlar kiberhujumga javoban qonuniy chora ko‘rish, jumladan javob choralari (kontrmeralar) qo‘llash imkoniyatiga ega. Ammo bunday choralar mutanosib bo‘lishi va xalqaro huquq talablariga muvofiq amalga oshirilishi shart. Atributsiyaning ishonchli asoslanmaganligi noqonuniy javob choralariga va xalqaro nizolarning kuchayishiga olib kelishi mumkin. Shu sababli xalqaro hamjamiyat kybersohada davlatlarning mas’uliyatli xatti-harakati normalarini, ishonch chora-tadbirlarini va nizolarni tinch yo‘l bilan hal etish mexanizmlarini rivojlantirishga intilmoqda.

Xulosa qilib aytganda, kiberhujumlar uchun davlatlarning xalqaro-huquqiy javobgarligi zamonaviy xalqaro huquqning shakllanib borayotgan, ammo hal etilmagan muammolarga boy sohasidir. Amaldagi umumiy normalar kybersohaga tatbiq etilsa-da, atributsiya, mutanosiblik va javob choralari bilan bog‘liq masalalar aniq huquqiy tartibga solishni taqozo etadi. Bu boradagi xalqaro hamkorlikni chuqurlashtirish, umumiy qoidalar va mexanizmlarni ishlab chiqish global kiberxavfsizlikni ta’minlashning zaruriy shartidir.

ADABIYOTLAR RO‘YXATI:

1. Davlatlarning xalqaro nomaqbul xatti-harakatlar uchun javobgarligi to‘g‘risidagi moddalar (BMT Xalqaro huquq komissiyasi, 2001).
2. Birlashgan Millatlar Tashkiloti Nizomi (San-Fransisko, 1945).

3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.
4. BMT hukumat ekspertlari guruhining axborot xavfsizligi bo'yicha hisobotlari (UN GGE, 2015; 2021).