KIBERHUJUMLAR VA XALQARO HUQUQ: DAVLATLARNING MAS'ULIYATI MASALASI

Sobirjonova E'zoza Olimjon qizi
Toshkent davlat yuridik universiteti talabasi

Annotatsiya: Ushbu maqolada kiberhujumlarning turlari, kiberhujumlar va xalqaro huquq doirasida davlatlarning xalqaro-huquqiy javobgarligi, davlatlarning mas'uliyati masalasi tahlil qilinadi. Maqolada kibermakonda sodir etiladigan hujumlarning huquqiy tabiati, kibermakon tushunchasi, kiberhujumlar va davlatlarning javobgarligiga oid real holatlar o'rganiladi. Shuningdek, maqolada davlatlarning kiberhujumlar uchun javobgarligini belgilashdagi asosiy muammolar, normativ noaniqlik va amaliy mexanizmlardagi bo'shliqlar yoritiladi. Tadqiqot natijalariga ko'ra, kibermakonda samarali huquqiy tartibni ta'minlash uchun xalqaro hamkorlikni kuchaytirish, yagona huquqiy mezonlarni ishlab chiqish va javobgarlik mexanizmlarini takomillashtirish lozimligi ta'kidlanadi.

Kalit so'zlar: Kiberhujum, aktiv hujum, passiv hujum, DDoS, Sniffing, Phishing, Malware, Key Loggers.

CYBERATTACKS AND INTERNATIONAL LAW: THE ISSUE OF STATE RESPONSIBILITY

Tashkent State University of Law
2nd-year student of the Faculty of Public Law

Abstract: This article analyzes the types of cyberattacks, cyberattacks within the framework of international law, and the issue of international legal responsibility of states. The article examines the legal nature of attacks occurring in cyberspace, the concept of cyberspace, and real cases related to cyberattacks and state responsibility. It also highlights the main problems in determining state responsibility for cyberattacks, including normative uncertainty and gaps in practical mechanisms. Based on the research results, it is emphasized that strengthening international cooperation, developing unified legal standards, and improving accountability mechanisms are necessary to ensure effective legal regulation in cyberspace.

Keywords: Cyberattack, active attack, passive attack, DDoS, Sniffing, Phishing, Malware, Key loggers.

КИБЕРАТАКИ И МЕЖДУНАРОДНОЕ ПРАВО: ВОПРОС ОТВЕТСТВЕННОСТИ ГОСУДАРСТВ

Ташкентский государственный юридический университет
Студент 2 курса факультета публичного права

Аннотация: В данной статье анализируются виды кибератак, кибератаки в рамках международного права, а также вопрос международно-правовой ответственности государств. В статье рассматриваются правовая природа атак, совершаемых в киберпространстве, понятие киберпространства, а также реальные случаи, связанные с кибератаками и ответственностью государств. Кроме того, освещаются основные проблемы определения ответственности государств за кибератаки, включая нормативную неопределенность и пробелы в практических механизмах. По результатам исследования подчеркивается необходимость усиления международного сотрудничества, разработки единых правовых стандартов и совершенствования механизмов ответственности для обеспечения эффективного правового регулирования в киберпространстве.

Ключевые слова: Кибератака, активная атака, пассивная атака, DDoS, сниффинг, фишинг, вредоносное ПО, кейлоггеры.

I. Kirish

Axborot texnologiyalarining jadal suratlar bilan tez rivojlanishi insoniyat hayotining barcha sohalarini tubdan o‘zgartirmoqda. Raqamli transformatsiya davlat boshqaruvi, iqtisodiyot, moliya, sog‘liqni saqlash va hatto harbiy tizimlarni ham chetlab o’tmasdan, chuqur kirib bormoqda. Shu bilan bir qatorda, bu jarayon yangi tahdidlarni, xususan, kiberhujumlar va kiberjinoyatlar xavfini yuzaga keltirdi. Bugungi kunda kiberhujumlar nafaqat individual shaxslar yoki kompaniyalarga, balki butun davlatlarning xavfsizligiga hamda insoniyatning taqdiriga ham jiddiy tahdid solmoqda. Kiberhujumlar orqali davlat infratuzilmasiga zarar yetkazish, saylov tizimlariga aralashish va ziyon berish, maxfiy ma’lumotlarni o‘g‘irlash kabi holatlar tobora ko‘payib bormoqda. Shuning uchun, xalqaro huquqda davlatlarning kiberhujumlar bilan bog‘liq javobgarligi masalasi dolzarb muammolardan biriga aylanib bormoqda.

Maqolaning asosiy maqsadi – kiberhujumlarning xalqaro huquq nuqtai nazaridan baholanishi, davlatlarning bu boradagi mas’uliyati, mavjud huquqiy mexanizmlar, shuningdek ularning samaradorligini tahlil qilishdan iborat.

II. Metodologiya

Ushbu tadqiqot quyidagi ilmiy metodlarga asoslanadi:

Tahliliy metod – xalqaro huquqiy normalar va hujjatlarni o‘rganish va tahlil qilish;

Taqqoslash metodi – turli davlatlar amaliyotini bir-biri bilan solishtirish;

Normativ-huquqiy tahlil – xalqaro huquqiy hujjatlar, jumladan BMT rezolyutsiyalari, davlat javobgarligi to‘g‘risidagi maqolalar va doktrinalarni o‘rganish;

Case study (holat tahlili) – real kiberhujumlar misolida ko’rib chiqish;

Shuningdek, ilmiy maqolalar, xalqaro tashkilotlar hisobotlari va ekspert xulosalaridan ham foydalanildi.

III. Natijalar

Kiberhujum nima va ularning turlari.

Kiberhujum - bu maxfiy ma'lumotlarni olish, zarar yetkazish yoki boshqa noqonuniy yo'l bilan amalga oshiriluvchi kompyuter tizimi yoki tarmog'iga qilingan hujumdir. Kiberhujum tarmoqqa, kompyuter tizimiga yoki raqamli qurilmalarga ruxsatsiz kirish orqali ma’lumotlar va boshqa aktivlarni o’g’irlash, ularni fosh qilish, o’zgartirish yoki yo’q qilishga qaratilgan qasddan sodir etilgan har qanday harakatdir. Kiberhujumlarga asosan shaxsiy, jinoiy yoki siyosiy motivlar sabab bo’ladi. Shaxsiy norozilik yoki moddiy manfaatlar evaziga odatda tizimlarga kirish va ma’lumotlardan foydalanish huquqiga ega insayderlar tomonidan amalga oshiriluvchi hujumlar misol bo’la oladi. Kiberjinoyatchilar esa ruxsat etilmagan kirish orqali pul og’irlash, ma’lumotlarni o’g’irlash yoki biznesni buzish orqali moliyaviy foyda olishga intiladi. Kiberhujum qiluvchilar odatda kompyuter tarmoqlari orqali tizimga kirishga urinib, quydagilardan biror bir maqsadga erishishga harakat qilishadi:

- Pul;
- Mijozlar ro’yxati;
- Korxona va tashkilotlarning moliyaviy ma’lumotlari;
- Elektron pochta manzillari va kirish ma’lumotlari;
- Tijorat sirlari yoki mahsulot dizayni kabi intellectual mulk;
- Axborot tizimlari yoki tarmoq infratuzilmasini buzish.

Kiberhujumlarning turlari ko`p bo'lib, eng keng tarqalganlari bular-DDoS va fishingdir.

DDoS (Distributed Denial of Service) hujumi — bu veb-sayt yoki onlayn xizmatni vaqtinchalik yoki butunlay ishdan chiqarish uchun qilinadigan hujum. Hujumchilar buzilgan qurilmalar orqali bir saytga birdaniga juda katta hajmda so‘rov (trafik) yuborishadi. Natijada sayt ortiqcha yuklama sabab ishlashdan to‘xtab qoladi yoki juda sekinlashadi.

Fishing — jinoyatchilar tomonidan odamlarni aldash orqali parol, karta raqami yoki boshqa shaxsiy ma’lumotlarni qo‘lga kiritish usullari. Ular o‘zlarini bank yoki ishonchli tashkilot nomidan xabar yuborib, sizdan maxfiy ma’lumot so‘rashadi. Bu ko‘pincha telefon qo‘ng‘iroq, e-mail, SMS yoki ijtimoiy tarmoqlarda bo‘ladi.

Malware (zararli dasturiy ta’minot) – kompyuter tizimlarini zararlash, nazorat qilish yoki ularga zarar yetkazish uchun yaratilgan dastur hisoblanadi.

Kiberhujumlar asosan ikki turga bo’linadi, bular:

1. Passiv hujumlar;
2. Aktiv hukumlar.

Passiv hujumlarda hujum kriptografik protokol yoki kriptotizmga qaratilgan hujum hisoblanadi, bunda buzg'unchi uzatiladigan shifrlangan xabarlarni kuzatadi va ulardan foydalanadi, ammo qonuniy foydalanuvchilarning xatti-harakatlariga ta'sir qilmaydi. Buzg'unchining bu kabi holatlarda maqsadi uzatilayotgan axborotni olish hisoblanadi. Aktiv hujum bu buzg'unchi tizimga aralashib, ma'lumotlarni o'zgartirish, yo'q qilish yoki to'sqinlik qilishga urinadigan hujum hisoblanadi. Bu kabi hujumlar tizimning butunligi va mavjudligiga tahdid soladi. Passiv hujumning "Traffic Analysis", "Sniffing", "Key Loggers" kabi turlari keng tarqalgan.

Trafik tahlili hujumi (Traffic Analysis) – bu tarmoq orqali uzatilayotgan ma'lumotlarni dekodlash yoki to'g'ridan-to'g'ri o'qib olish o'rniga, ularninng chastotasi, harakati, hajmi va yo'nalishini tahlil qilish orqali maxfiy ma'lumotlarni aniqlashga qaratilgan kiberhujum.

Xabarlarni ochib ko'rish hujumi (Release of messege) – bu tarmoqdagi aloqa jarayonida maxfiy yoki shaxsiy ma'lumotlarni ruxsatsiz eshitish yoki o'qish orqali amalga oshiriladigan kiberhujum.

Sniffing hujumi – bu tarmoq orqali uzatilayotgan ma'lumotlarni maxfiy ravishda tutib olish va tahlil qilishga qaratilgan kiberhujum. Bu hujum orqali hujumchi foydalanuvchilarning login ma'lumotlari, parollari, bank rekvizitlari va boshqa shaxsiy ma'lumotlarini qo'lga kiritishi mumkin.

Xalqaro huquq prinsiplari va kibermakon.

Avvalo, Kibermakon nima ekanligiga to'xtalib o'tsak. *Kibermakon* — bu informatsion texnologiyalar yordamida yaratilgan va global tarmoq orqali ulanish imkonini beruvchi virtual muhitdir. U insonlar, tashkilotlar va davlatlar o'rtasida axborot almashish, ma'lumotlar uzatish va aloqalar o'rnatish uchun muhim platforma hisoblanadi.

Zamonaviy xalqaro huquq asosan davlatlar o‘rtasidagi munosabatlarni tartibga solishga qaratilgan bo‘lib, uning asosiy tamoyillari uzoq tarixiy rivojlanish jarayonida shakllangan deya olamiz. Biroq, raqamli texnologiyalarning juda keskin rivojlanishi va kibermakonning global miqyosda kengayib borishi ushbu an'anaviy prinsiplarning yangi sharoitlarda qay darajada qo‘llanishi masalasini muammo sifatida olib chiqdi.

Avvalo, xalqaro huquqning eng muhim tamoyillaridan biri hisoblanadigan davlat suvereniteti prinsipi kibermakonda ham asosiy o‘rinni egallaydi. Suverenitet so'zi davlatning o‘z hududi va ichki ishlariga nisbatan to‘liq va mustaqil vakolatga egaligini anglatadi. An'anaviy talqinda bu hududiy yaxlitlik hamda siyosiy mustaqillik bilan bog‘liq bo‘lsa, zamonaviy yondashuvda kiber infratuzilma ham davlat hududining funksional elementlaridan biri sifatida qaralmoqda. Demak, boshqa davlat tomonidan ruxsatsiz ravishda biror davlatning axborot tizimlariga kirish, ularni buzish yoki boshqaruv tizimlariga ta'sir ko‘rsatish suverenitetning buzilishi sifatida baholanishi ham mumkin. Ilmiy adabiyotlarda suverenitetning kibermakondagi qo‘llanishi

bo‘yicha ikki asosiy yondashuv mavjudligini ko’rishimiz mumkin. Birinchi yondashuvga ko‘ra, har qanday ruxsatsiz kiber aralashuv suverenitetga ta’sir qiladi va uni buzadi. Ikkinchi yondashuv esa faqatgina sezilarli zarar yoki jiddiy oqibatlarga olib kelgan holatlarnigina suverenitet buzilishi hisoblaydi. Amaliyotda davlatlar ko‘proq ikkinchi yondashuvga moyil bo‘lib, bu esa huquqiy noaniqliklarni yuzaga keltiradi.

Keyingi muhim prinsip – kuch ishlatmaslik (prohibition of the use of force) prinsipidir. Ushbu prinsip Birlashgan Millatlar Tashkiloti Nizomining 2-moddasi 4-bandida mustahkamlab qo‘yilgan bo‘lib, davlatlar o‘rtasida kuch ishlatishni yoki kuch bilan tahdid qilishni taqiqlaydi. Kibermakonda ushbu prinsipning qo‘llanishi murakkab masalalardan biri hisoblanadi. Eng asosiy savol shundan iboratki, qachon kiberhujum “kuch ishlatish” darajasiga yetadi? Ilmiy nazariyalarda keng tarqalgan yondashuvga ko‘ra, agar kiberhujum jismoniy zarar keltirsa yoki an’anaviy qurolli hujum bilan tenglashtiriladigan darajada oqibatlar keltirib chiqarsa (masalan, elektr stansiyalarining ishdan chiqishi, transport tizimining falajlanishi, insonlar hayotiga xavf tug‘ilishi), u holda bunday harakat kuch ishlatish sifatida baholanishi mumkin. Biroq, faqat ma’lumotlarni o‘g‘irlash yoki vaqtinchalik tizim buzilishlari odatda ushbu mezonlarga kirmaydi. Shuningdek, qurolli hujum (armed attack) tushunchasi ham muhim ahamiyatga ega. Agar kiberhujum qurolli hujum sifatida tan olinadigan bo’lsa, jabrlangan davlat o‘zini himoya qilish huquqiga ega bo‘ladi. Ammo, bu mezonni aniqlash juda ham murakkab, chunki kiberhujumlarning aksariyati an’anaviy qurolli hujum darajasiga yetmasligi mumkin. Shuning uchun, xalqaro huquqda “threshold” masalasi – ya’ni qaysi darajadan boshlab kiberhujum qurolli hujum hisoblanishi – haligacha bahsli masala bo‘lib kelmoqda.

Keyingi asosiy prinsip – davlatlarning ichki ishlariga aralashmaslik (non-intervention). Bu prinsip bir davlat boshqa davlatning siyosiy, iqtisodiy yoki ijtimoiy tizimlariga majburlov yo‘li bilan aralasha olmasligini bildiradi. Kibermakonda bu prinsip ayniqsa saylov jarayonlariga aralashuv, siyosiy kampaniyalarga ta’sir ko‘rsatish yoki ijtimoiy fikrni manipulyatsiya qilish yordamida buzilishi mumkin. Masalan, boshqa davlatning saylov tizimiga kiber aralashuv demokratik jarayonlarga bevosita tahdid sifatida baholanib, xalqaro huquqni buzadi.

Xalqaro huquqning yana bir muhim jihati – davlatlarning zarar yetkazmaslik majburiati (due diligence)dir. Bu prinsipga binoan, davlat o‘z hududidan boshqa davlatlarga zarar yetkazilishining oldini olish uchun barcha zarur choralarni ko‘rishi darkor. Kibermakonda bu shuni bildiradiki, davlat o‘z hududida joylashgan serverlar yoki infratuzilmalardan boshqa davlatlarga qarshi kiberhujumlar amalga oshirilishiga yo‘l qo‘ymasligini nazorat qilishi lozim. Agar davlat bunday harakatlarni bilib turib oldini olmasa, u xalqaro-huquqiy javobgarlikka tortilishi ham mumkin. Ammo, amaliyotda bu majburiyatni qo‘llash ham murakkab masala. Chunki, davlatlar har doim

ham o‘z hududidagi barcha kiber faoliyatlarni to‘liq nazorat qila olish imkoniga ega emas. Bundan tashqari, texnik imkoniyatlar va resurslar ham turli davlatlarda turlicha.

Umuman olganda, xalqaro huquqning asosiy prinsiplari kibermakonda ham amal qilib kelmoqda, biroq ularning qo‘llanishi bir qator muammolar bilan to‘qnash kelmoqda.

Davlatlarning xalqaro-huquqiy javobgarligi.

Kiberhujumlar masalasida davlatlarning xalqaro-huquqiy javobgarligi zamonaviy xalqaro huquqning eng murakkab va bahsli yo‘nalishlaridan biri hisoblanadi. An’anaviy xalqaro huquq davlatlar o‘rtasidagi munosabatlarni tartibga solishda aniq mexanizmlarni ishlab chiqqaniga qaramasdan, kibermakonning o‘ziga xos xususiyatlari – anonimlik, transmilliylik va tezkorlik – ushbu mexanizmlarning qo‘llanishini sezilarli darajada murakkablashtirmoqda. Shunga qaramasdan, hozirgi ilmiy va amaliy yondashuvlar shuni ko‘rsatmoqdaki, kiberhujumlar ham davlat javobgarligi to‘g‘risidagi umumiy xalqaro huquq normalari doirasida baholanishi mumkin. Ba’zi bir maqalolarga ko‘ra, davlat javobgarligining yuzaga kelishi uchun ikki asosiy element mavjud bo‘lishi darkor: birinchidan, xalqaro-huquqiy majburiyatning buzilishi; ikkinchidan, ushbu buzilishning davlatga tegishliligi, ya’ni atributsiyasi. Kiberhujumlar aynan mana shu ikki element nuqtai nazaridan baholanadi. Avvalo, xalqaro-huquqiy majburiyatning buzilishi masalasiga to‘xtalish kerak. Kiberhujumlar davlatlarning suverenitetini buzishi, kuch ishlatmaslik prinsipiga zid bo‘lishi yoki ichki ishlariga noqonuniy aralashuv darajasida baholanishi mumkin. Masalan, agar bir davlat boshqa davlatning energetika tizimiga kiberhujum uyushtirgan holda uni ishdan chiqarsa, bu nafaqat texnik zarar, balki xalqaro huquqning asosiy prinsiplari buzilishi sifatida ham ko‘rib chiqilishi mumkin. Ammo, xalqaro-huquqiy javobgarlikni aniqlashdagi eng murakkab bosqich – bu atributsiya (attribution)dir. Ya’ni, muayyan kiberhujumni aniq bir davlatga bog‘lash zarurati mavjuddir. An’anaviy xalqaro huquqda atributsiya nisbatan osonroq bo’ladi, kibermakonda bu jarayon nihoyatda murakkablashadi. Chunki, kiberhujumlar ko‘pincha anonym tarizda, botlar orqali yoki boshqa usullarda amalga oshiriladi. Bu esa hujum manbasini aniqlashni texnik va huquqiy jihatdan qiyinlashtirib yuboradi. Masalan, kiberjinoyat sodir etilsa, jinoyatchi bir davlatda, server boshqa bir davlatda, jabrlangan inson esa uchinchi bir boshqa davlatda bo’lishi mumkin. Xalqaro huquqqa binoan, agar kiberhujum davlat organlari tomonidan amalga oshirilsa yoki ular tomonidan nazorat qilinayotgan shaxslar tomonidan sodir etilsa, u holda bu harakat bevosita davlatga tegishli deb topiladi. Kiberhujumlarda yana bir muhim masala – bu davlatlarning “due diligence” majburiyatidir. Bu majburiyat bevosita hujumni amalga oshirishdan farqli ravishda “passiv javobgarlik” sifatida namoyon bo‘ladi. Davlat javobgarligining yana bir muhim jihati – bu xalqaro-huquqiy oqibatlar masalasi

hisoblanadi. Agar davlat kiberhujum orqali xalqaro majburiyatni buzgan deb topilsa, u holda u quyidagi majburiyatlarni bajarishi kerak:

Huquqbuzarlikni to‘xtatish;

Kelajakda takrorlanmasligini ta’minlash;

Yetkazilgan zararni qoplash (reparation).

Reparatsiya o‘z ichiga restitusiyani (avvalgi holatni tiklash), kompensatsiyani (moddiy zarar uchun to‘lov) va satisfaksiyani (rasmiy uzr yoki boshqa shakldagi qoniqtirish) olishi ham mumkin. Kiberhujumlar holatida ayniqsa kompensatsiya masalasi dolzarb hisoblanadi, sababi zarar ko‘pincha iqtisodiy va infratuzilmaviy yo‘qotishlar bilan bog‘liq bo‘ladi. Qo’shimchasiga shuni aytishimiz joizki, xalqaro huquqda qarshi choralar instituti ham mavjud bo’lib, agar bir davlat kiberhujumdan zarar ko‘rsa, u xalqaro huquq doirasida boshqa davlatga nisbatan proporsional va vaqtinchalik choralar ko‘rishi ham mumkin.

Amaliy holatlar: kiberhujumlar va davlat javobgarligi.

1. Estoniya kiberhujumi (2007)

Estoniya davlati 2007-yil 27-apreldan boshlab tarixdagi eng yirik kiberhujumlardan biriga duch keladi. Bu hujumlar Estoniyaning davlat organlari, bank tizimi, ommaviy axborot vositalari, gazetalari va boshqa muhim infratuzilmalariga qarshi amalga oshiriladi. Aholiga sezilarli darajada ta’sir ko‘rsatgan hujumlarning aksariyati DDoS turiga mansub bo‘lib, ular oddiy foydalanuvchilarning “ping flood” kabi usullaridan tortib, odatda spam tarqatishda ishlatiladigan qimmat botnetlarni ijaraga olishgacha bo‘lgan vositalar orqali amalga oshirilgan. Shuningdek, yirik yangilik portallarining izoh bo‘limlariga spam yuborish va saytlarni buzish (masalan, Estoniya Islohotlar partiyasi saytini) holatlari ham kuzatilgan. Ba’zilar bu hujumlarni ilgari kuzatilmagan darajadagi murakkablikka ega deb baholagan. 2008-yil yanvarda, bir nafar Estoniya fuqarosi ayblanib, sudlangan.2009-yil 10-mart kuni esa Konstantin Goloskokov (Kremlga yaqin “Nashi” yoshlar harakati a’zosi) hujum uchun javobgarlikni o‘z zimmasiga olgan. Ushbu misolni tahlil qiladigan bo’lsak, asosiy muammo atributsiya bo‘ldi. Hujumni davlat bilan bog‘lash uchun yetarli dalillar mavjud emasdi. Hujumlar jiddiy iqtisodiy zarar keltirib chiqargan bo‘lsa ham, ular “qurolli hujum” darajasiga yetmagan deb baholandi. Ahamiyatli tomoni shundaki bu holat xalqaro huquqda kiberhujumlarni tartibga solish zarurligini ko‘rsatgan ilk signal vazifasini bajardi.

2. Stuxnet operatsiyasi (2010)

Stuxnet — bu zararli kompyuter qurti (virus) bo‘lib, u ilk bor 2010-yil 17-iyunda aniqlangan va kamida 2005-yildan boshlab ishlab chiqilgan hisoblanadi. Stuxnet sanoat boshqaruv tizimlari, ya’ni SCADA systemsni nishonga oladi va 2009-yilda Natanz Nuclear Facilitydagi kompyuterga o‘rnatiladi va Eron yadroviy dasturiga katta zarar yetkazgan. Garchi AQSH ham, Isroil ham bu hujum uchun rasmiy javobgar hisoblanmagan bo‘lsa-da, ko‘plab mustaqil ommaviy axborot vositalari Stuxnetni

ushbu ikki davlat tomonidan birgalikda ishlab chiqilgan kiberhujum deb hisoblagan. Bu hamkorlik Operation Olympic Games nomi bilan tanilgan. Bu holat “kuch ishlatish” yoki hatto “qurolli hujum” sifatida baholanishi mumkin. Agar davlat ishtiroki to‘liq isbotlansa, bu xalqaro huquqning jiddiy buzilishi hisoblash mumkin.

3. **Ukraina elektr tarmog‘iga hujum (2015)**

Kiberhujum 2015-yilda Ukraina elektr ta’minot tizimiga uyushtirildi. Natijada yuz minglab odamlar bir necha soat davomida elektrsiz qoladi. Bu hujum “BlackEnergy” zararli dasturi orqali amalga oshirilgan edi. Ko‘plab xalqaro ekspertlar fikricha ushbu hujum ortida Rossiyaga aloqador guruhlar turgan. Lekin aniq javobgar mavhum bo’lib qolgan. Bu hujum kritik infratuzilmaga bevosita kuchli zarar yetkazgan. Agar davlat ishtiroki tasdiqlansa, bu kuch ishlatish prinsipining buzilishi hisoblanardi. Shuningdek, bu holat due diligence majburiyatlarini ham muhokamaga olib chiqardi. Ahamiyatli tomoni shundaki, bu voqea kiberhujumlar real hayotga qanday jiddiy zarar yetkazishini amalda ko‘rsatdi.

IV. Muhokama

Kiberhujumlar masalasida davlatlarning xalqaro-huquqiy javobgarligi masalasi shuni ko‘rsatadiki, muammo xalqaro huquq normalarining yo‘qligida emas, balki ularning amaliy qo‘llanishidagi tizimli nomuvofiqlik borligidadir. Mavjud huquqiy prinsiplar nazariy jihatdan kibermakonga tatbiq etilishi mumkin bo‘lsa-da, amaliyotdaularni qo’llashda muammolar bor. Quyida biz ushbu muammolarni muhokama qilib, sabablariga to’xtalib yechimlar berishga harakat qilamiz. Birinchi muammo bu - javobgarlik chegarasining noaniqligi. Zamonaviy kiberoperatsiyalar va kiberhujumlar ko‘pincha “qurolli hujum” chegarasidan past darajada amalga oshiriladi. Bu holat xalqaro huquqda aniq belgilanmagan va taqiqlanmagan, biroq zararli bo‘lgan faoliyatni o‘z ichiga oladi. Davlatlar o‘rtasida kiberhujumlarning aniq huquqiy chegaralari bo‘yicha yagona kelishuv yo’q. Yechim sifatida shuni keltirish mumkinki, kiberhujumlarning qaysi darajadan boshlab “kuch ishlatish” yoki “qurolli hujum” hisoblanishini aniq belgilovchi xalqaro standartlar ishlab chiqilishi va javobgarliklar aniq belgilanishi darkor. Bu masalada Tallinn qo‘llanmasi muhim asos bo‘lib xizmat qilishi mumkin, biroq uni majburiy huquqiy hujjatga aylantirish masalasi ko‘rib chiqilishi lozim. Keyingi muammo Atributsiya (attribution) mexanizmining zaifligidir. Davlatlar javobgarligining asosiy sharti – hujumni aniq bir davlatga bog‘lash hisoblanadi. Sababi texnologik murakkablik va isbot standartlarining yo‘qligidir. Yechim sifatida mustaqil xalqaro ekspertlar yoki tashkilotlar asosida ishlovchi atributsiya markazlarini tashkil etishni taklif etish mumkin. Bu tizim texnik va huquqiy dalillarni jamlagan holatda obyektiv xulosalar berishi mumkin. Keyingi yana bir muammo javobgarlik va jazolash mexanizmlarining samarasizligidir. Zamonaviy amaliyotda davlatlar qo’llaydigan javobgarlik choralari ko‘pincha huquqiy emas, balki siyosiy xarakterga ega. Ushbu muammoni hal qilish uchun kiber nizolarni ko‘rib

chiqadigan maxsus xalqaro organ (masalan, kiber arbitraj sudi) tashkil etilishi mumkin. Bu organ davlatlar o‘rtasidagi nizolarni huquqiy asosda hal qilish imkonini yaratadi.

V. Xulosa

Kiberhujumlar zamonaviy xalqaro munosabatlarda davlatlar xavfsizligiga bevosita ta’sir ko‘rsatuvchi eng muhim tahdidlardan biri hisoblanmoqda. Ular xalqaro huquq nuqtai nazaridan hal qilish murakkab bo’lgan muammolarni keltirib chiqarib, ayniqsa davlatlarning javobgarligi masalasini murakkablashtirmoqda. Tahlillar shuni ko‘rsatadiki, mavjud xalqaro huquq prinsiplari kibermakonga tatbiq etilishi mumkin bo‘lsa-da, amaliyotda ularning qo‘llanilishida bo’shliqlar va murakkabliklar mavjud.

Shuning uchun, kiberhujumlar bo‘yicha xalqaro hamkorlikni kuchaytirish, huquqiy mezonlarni aniqlashtirish va davlatlar o‘rtasida yagona yondashuvni shakllantirish muhim ahamiyat kasb etadi. Faqat shundagina kibermakonda samarali va barqaror xalqaro huquqiy tartibga erishish mumkin. Xulosa qilib aytganda, biz tadqiqot davomida ushbu muammolarni o’rganib, sabablariga to’xtalib, ularga yechimlar berish bilan birgalikda, amaliy misollar va holatlarni ham ko’rib chiqdik.

Foydalanilgan adabiyotlar:

1. Kiberjinoyat huquqi [Matn]: o‘quv qo‘llanma / G‘ulommamatova Parvina Akbarali qizi. – T.: TDYU nashriyoti, 2025. – 144 b.
2. Kiber huquq [matn]: o‘quv qo‘llanma / Abdixakimov Islombek Bahodir og ‘li – T.: TDYU nashriyoti, 2025. – 418 b.
3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020. – 1248 p.
4. S Bozorov, N Akhmedova, D Qurbonaliyeva, K Gultekin, Survey on honeypot: Detection, countermeasures and future with MI. AIP Conference Proceedings, 2024. Doi.org/10.1063/5.0242098
5. https://research-repository.griffith.edu.au/server/api/core/bitstreams/e6e5408e-5ff9-5afb-bd29-e54ba1cc932b/content
6. https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf
7. https://najottalim.uz/blog/kiberhujumlarning-turlari?srsltid=AfmBOoo9NgvCV7HuBFQPtHaMc0Fv08jl__dnTRpBIQXm9t-v36-kMJD8
8. https://italent.uz/blog/kiberhujumlar-nima-u-va-undan-qanday-himoyalanish-mumkin
9. **https://uz.wikipedia.org/wiki/Stuxnet**
10. https://cyberleninka.ru/article/n/kiberhujumlar-va-ularni-amalga-oshirish-usullari/viewer
11. https://casebook.icrc.org/case-study/international-law-commission-articles-state-responsibility