IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 22 Issue 01 IYUN 2026

KIBER XAVFSIZLIK VA XALQARO HUQUQ: VIRTUAL URUSHLAR TAHDIDI

Berdiyeva Elshoda Elmanovna
Turon universitetining Xalqaro munosabatlar yo'nalishining
1-kurs talabasi

ANNOTATSIYA: Hozirgi davrda axborot texnologiyalarining jadal rivojlanishi jamiyat hayotini tubdan o'zgartirdi. Internet, mobil tarmoqlar va bulutli xizmatlar orqali iqtisodiyot, ta'lim, siyosat va hatto xavfsizlik tizimlari ishlaydi. Shu bilan birga, texnologik rivojlanish yangi xavf-xatarlarni ham keltirib chiqarmoqda. Kiberxavfsizlik hozirgi global muhitda xavfsizlikning markaziy unsuriga aylandi. Ushbu maqolada kiberxavfsizlik tushunchasi, virtual urushlar tahdidi va ularning xalqaro huquq tizimidagi o'rni tahlil qilinadi. Maqsad — o'quvchi uchun mavzuni sodda, tushunarli hamda amaliy misollar orqali ochib berish.

Kalit so'zlar : kiberxavfsizlik; xalqaro huquq; virtual urush; kiberhujum; axborot xavfsizligi; davlat suvereniteti; Budapesht konvensiyasi.

KIRISH

XXI asr axborot texnologiyalari asri deb ataladi. Har kuni kompyuterlar, smartfonlar, serverlar va tarmoqlar orqali milliardlab ma'lumotlar almashinadi. Bu jarayon hayotimizni yengillashtirdi, lekin shu bilan birga yangi xavf va muammolarni ham keltirib chiqardi. Kiberxavfsizlik atamasi bugungi kunda ko'plab sohalarda — davlat boshqaruvida, bank tizimlarida, sanoatda va sog'liqni saqlashda dolzarb muammo sifatida qaralmoqda.

Kiberxavfsizlik shunchaki viruslardan himoya emas; bu kengroq tushuncha — ma'lumotlarni, tizimlarni, infratuzilmalarni, shuningdek, insonlarning shaxsiy hayotini himoya qilishni o'z ichiga oladi. Davlatlar va tashkilotlar raqamli maydonni strategik resurs sifatida ko'rmoqda. Shu sababli, kiberhujumlar va virtual urushlar xalqaro munosabatlarga, xalqaro huquqqa ta'sir qilmoqda.

Virtual urushlar orqali davlatlar yoki boshqa aktorlar siyosiy va iqtisodiy maqsadlarga erishish uchun axborot va kommunikatsiya tizimlariga zarar yetkazadi. Bu yangi hujum shakli aniq bo'lmagan manbadan keladi, manbasini aniqlash qiyin, oqibatlari esa ko'pincha juda jiddiy bo'ladi. Xalqaro huquq esa hozircha kiberfazoni to'liq va aniq tartibga solgan emas. Shu nuqtai nazardan ushbu maqola mavzuni sodda talaba uslubida tushuntirishga urinadi.

ADABIYOTLAR TAHLILI VA METODLAR

Kiberxavfsizlik bo'yicha ko'plab tadqiqotlar, hisobotlar va xalqaro hujjatlar mavjud. Asosiy hujjatlardan biri — Budapesht konvensiyasi (2001), u kiberjinoyatlarga qarshi kurashish bo'yicha asosiy huquqiy mexanizmdir. NATOning Tallin qo'llanmalari (Tallinn Manual) ham kiberurush holatlarida xalqaro huquq qanday qo'llanilishi mumkinligi haqida ekspert fikrlarini jamlaydi. BMT rezolyutsiyalari esa axborot va telekommunikatsiyalar sohasida xalqaro xavfsizlikni muhokama qiladi.

Maqolada ishlatilgan metod — tahliliy va qiyosiy yondashuv: mavjud xalqaro hujjatlar, bir qator real voqealar (Stuxnet, Estoniya hujumi, Rossiya–Ukraina kiberhujumlari) va mamlakatlarning milliy strategiyalari (AQSh, Rossiya, Xitoy, O'zbekiston) tahlil qilindi. Bundan tashqari, mavzu bo'yicha ommaviy axborot manbalari va ilmiy maqolalar yordami bilan umumiy natijalar chiqarildi. Maqola empirik tadqiqot emas, balki mavjud manbalarni jamlab, sodda tilda tushuntirishga qaratilgan.

NATIJALAR VA MUHOKAMA

1. Kiberxavfsizlikning hozirgi holati

Bugungi kunda kiberxavfsizlik butun dunyo bo‘ylab e’tibor markazida. Davlatlar axborot infratuzilmasini himoya qilish uchun maxsus tashkilotlar, qoidalar va strategiyalar ishlab chiqmoqda. Masalan, AQShda Cyber Command, NATOda Cooperative Cyber Defence Centre (Tallinn), Yevropa Ittifoqida esa muayyan strategiyalar mavjud. O‘zbekiston ham o‘z navbatida Axborot xavfsizligini ta’minlash bo‘yicha strategik hujjatlarni qabul qildi va markazlarni tashkil etdi. Bu holat kiberxavfsizlikning milliy darajada ham, xalqaro darajada ham muhimligini ko‘rsatadi.

2. Virtual urushlar misollari va ta’siri

Virtual urush va kiberhujumlar misolida bir necha taniqli voqealarni ko‘rsatish mumkin. 2010-yilda Eronning yadro obyektlariga ta’sir ko‘rsatgan Stuxnet virus hodisasi — kiberhujumning sanoat ob’ektlariga qanday zarar yetkazishi mumkinligini ko‘rsatdi. 2007-yilda Estoniyada davlat tizimlariga qarshi amalga oshirilgan DDoS hujumlari davlat faoliyatini to‘xtatib qo‘ygan va kiberxavfsizlik bo‘yicha xalqaro munosabatlarni keskinlashtirgan. 2016-yilda AQShdagi saylovlarga ta’sir qilgan holatlar va 2022-yildan keyingi Rossiya–Ukraina mojarosida kiberhujumlar keng qo‘llangan.

Bu hujumlar nafaqat texnik jihatdan, balki siyosiy va iqtisodiy jihatdan ham katta oqibat olib keladi: bank tizimlariga zarar yetkazilishi iqtisodiyotga putur beradi; elektr tarmoqlari to‘xtasa, sanoat va kommunal xizmatlar zarar ko‘radi; saylov tizimlariga aralashish esa demokratiyaga putur yetkazadi. Shunday qilib, virtual urushlar real dunyoda jiddiy natijalarga olib kelishi mumkin.

3. Xalqaro huquq va muammolar

Xalqaro huquq doirasida kiberhujumlarning maqomi hamon aniq belgilanmagan. BMT Nizomining 2-moddasidagi davlat suvereniteti va 51-moddadagi o‘zini oqlash huquqi kiberhujumlarga qanday tatbiq etilishini aniqlash qiyin. Agar kiberhujum to‘g‘ridan-to‘g‘ri jismoniy zarar yoki odam o‘limiga olib keladigan bo‘lsa, ba’zi ekspertlar uni qurolli hujum deb tan olish kerak, deb hisoblaydi. Ammo ko‘pchilik holatlarda zarar iqtisodiy yoki boshqaruv tizimlariga taalluqli bo‘ladi, shuning uchun qaror qabul qilish muammo tug‘diradi.

Boshqa muammo — hujum manbasini aniqlashdagi qiyinchilik. Kiberhujum anonim yoki proxy serverlar orqali o‘tkazilgani sababli bai‘nima davlatni ayblash qiyin. Bu holatda diplomatik aloqalarni buzish yoki noto‘g‘ri davlatni ayblash xavfi mavjud. Shu sababli xalqaro hamjamiyat holatlarni tekshirish, dalillarni yig‘ish va hamkorlik qilish mexanizmlarini yaratishi kerak.

4. Xalqaro hamkorlik va yechimlar

Hozirgi paytda xalqaro hamkorlik muhim yechimlardan biri hisoblanadi. Budapesht konvensiyasi a’zolari jinoyatlarni aniqlash va tergovda hamkorlik qilishmoqda. BMT doirasida esa axborot xavfsizligini ta’minlash bo‘yicha tavsiyalar va rezolyutsiyalar qabul qilinadi. NATO va YEXHT kabi tashkilotlar kibermudofaa bo‘yicha treninglar va tadbirlar o‘tkazadi.

Shuningdek, davlatlar o‘zaro ishonch va ochiqlikni oshirishga intilmoqda: ma’lumot almashish, tezkor ogohlantirish tizimlari, vaqti-vaqti bilan security drill (savunma mashqlari) orqali tajriba almashish. Texnik jihatdan esa — tizimlarni zamonaviylashtirish, xavfsizlik protokollarini joriy etish, mutaxassislarni tayyorlash va fuqarolarni axborot madaniyati bilan ta’minlash zarur.

5. Milliy tajriba (O‘zbekiston misoli)

O‘zbekiston so‘nggi yillarda raqamli transformatsiyaga katta e’tibor qaratmoqda. Elektron hukumat, onlayn xizmatlar, va raqamli iqtisodiyot rivojlanmoqda. Shu bilan birga, milliy qonunchilik va tashkilotlar ham shakllantirildi: axborot xavfsizligini ta’minlashga oid qonunlar qabul qilindi, markazlar tashkil etildi va oliy ta’limda mutaxassislar tayyorlanmoqda. Bular muhim qadamlar, lekin xalqaro hamkorlikni kengaytirish va tajriba almashish orqali natijalar samarali bo‘ladi.

6. Kelajakdagi tahdidlar: AI va IoT

Kelajakda sun’iy intellekt (AI) va Internet of Things (IoT) texnologiyalari kiberxavfsizlikni yangi bosqichga olib chiqadi. AI yordamida hujumlarni avtomatlashtirish yoki jarayonlarni manipulyatsiya qilish mumkin bo‘ladi. IoT qurilmalarning ko‘pligi esa hujum sirtlarini oshiradi — maishiy texnika, transport, tibbiy asbob-uskunalar ham tarmoqqa ulangan. Shu bois, bu yo‘nalishlar uchun maxsus standartlar va himoya choralari ishlab chiqilishi kerak.

XULOSA

Kiberxavfsizlik va virtual urushlar masalasi bugungi global dunyoning eng muhim muammolaridan biridir. Virtual hujumlar aniq davlat chegaralaridan o‘tib, iqtisodiy, siyosiy va ijtimoiy sohalarga katta zarar yetkazishi mumkin. Xalqaro huquq esa hozircha bu muammoga aniq va majburiy yechim bera olmayapti.

Bu vaziyat yangi xalqaro me’yorlarni ishlab chiqish, mavjud hujjatlarni yangilash va tartibga solish zaruratini tug‘diradi.

Davlatlar — o‘z milliy xavfsizligini mustahkamlash bilan bir qatorda, global hamkorlikni rivojlantirishi lozim. Budapesht konvensiyasi kabi hujjatlar bunga yaxshi boshlanish, ammo yetarli emas. Kelajak uchun tavsiyalar: birinchidan, kiberhujumlarni aniqlash va isbotlash uchun xalqaro hamkorlik mexanizmlarini kuchaytirish; ikkinchidan, texnik jihatdan himoya qilishni oshirish va mutaxassislar tayyorlash; uchinchidan, fuqarolar orasida axborot madaniyatini oshirish; va to‘rtinchidan, sun’iy intellekt va IoT xavfsizligi uchun xalqaro standartlar ishlab chiqish zarur.

Foydalanilgan adabiyotlar

1. Budapest Convention on Cybercrime, Council of Europe, 2001.
2. Tallinn Manual on the International Law Applicable to Cyber Warfare, NATO CCDCOE, 2013.
3. United Nations General Assembly Resolutions on Developments in the Field of Information and Telecommunications in the Context of International Security (turli yillar).
4. O‘zbekiston Respublikasi “Axborot xavfsizligini ta’minlash to‘g‘risida”gi Qonun, 2020.
5. Karimov B. Kiberxavfsizlik asoslari. Toshkent, 2021.
6. NATO Cyber Defence Report, annual reports.
7. Various news sources: BBC, Reuters, UN reports (2010–2024).