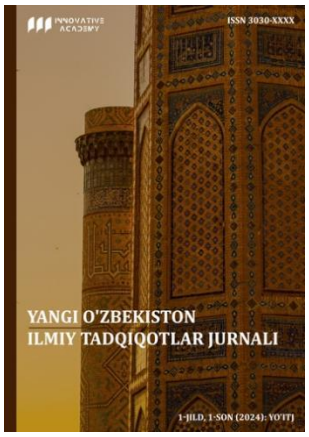


KIBERTERRORIZMGA QARSHI KURASHDA XALQARO HUQUQIY HAMKORLIK MEXANIZMLARI

Shodmonaliyeva Ruxshona Ikromjon qizi

Toshkent davlat yuridik universiteti Ommaviy huquq fakulteti 2-bosqich talabasi

ruxshonashodmonaliyeva09@gmail.com

https://doi.org/10.5281/zenodo.20268846

ARTICLE INFO

Qabul qilindi: 1-may 2026 yil
Ma'qullandi: 5-may 2026 yil
Nashr qilindi: 18-may 2026 yil

KEY WORDS

Kiberterrorizm, Kiberhujumlar, Xalqaro huquqiy hamkorlik, Budapest konvensiyasi, INTERPOL, Kiberxavfsizlik, Raqamli infratuzilma.

ABSTRACT

Kiberterrorizm internet va boshqa axborot-kommunikatsiya texnologiyalaridan foydalanib, tahdid qilish, qo'rqitish yoki zarar yetkazish orqali siyosiy yoki mafkuraviy maqsadlarga erishishga qaratilgan harakatlarni o'z ichiga oladi. Bunday hujumlarga ma'lumotlarni o'g'irlash, ma'lumotlarni manipulyatsiya qilish hamda muhim xizmatlarning faoliyatini izdan chiqarish kiradi. Raqamli infratuzilmaning jamiyat hayotida tobora muhim ahamiyat kasb etib borayotgani va zararli shaxslar uchun texnologiyalardan foydalanish imkoniyatlarining kengayib borayotgani sababli, kiberterrorizm global miqyosda jiddiy xavf sifatida namoyon bo'lmoqda. Shu sababli kiberterrorizmga qarshi samarali kurashish huquqni muhofaza qiluvchi organlar, davlatlar va xalqaro tashkilotlar o'rtasida keng ko'lamli hamkorlikni talab qiladi. Shu sababdan ushbu maqola kiberterrorizmga qarshi xalqaro huquqiy hamkorlik mexanizmlarini o'rganishga qaratilgan. Tadqiqotning maqsadi – kiberhujumlar va ularning global tahdidlari kontekstida davlatlar va xalqaro tashkilotlar tomonidan amalga oshirilayotgan huquqiy chora-tadbirlarni aniqlash, samaradorligini baholash va ilgari surish yo'llarini tahlil qilishdir. Metod sifatida maqolada huquqiy normativlar, xalqaro bitimlar va protokollar, shuningdek, so'nggi yirik kiberhujumlar (WannaCry, Yahoo, OPM, SolarWinds) holatlari tahlili qo'llanilgan. Tadqiqot orqali kiberterrorizmning turli davlatlar va infratuzilmalarga salbiy ta'siri, shu jumladan iqtisodiy zararlar, obro'ga putur yetishi va inson hayoti xavfi aniqlangan. Xulosalar shuni ko'rsatadiki, kiberterrorizmga samarali qarshi kurashish faqat xalqaro huquqiy me'yorlar va davlatlararo hamkorlik orqali mumkin bo'lib, u kiberhujumlarni tez aniqlash, ularga samarali javob berish va oldini olishda muhim ahamiyatga ega. Shu bilan birga, tadqiqot xalqaro hamkorlikni mustahkamlash va kiberxavfsizlik protokollarini modernizatsiya qilish zarurligini ham ta'kidlaydi.

KIRISH

Kiberterrorizm internet, axborot vositalari va aloqa platformalaridan terroristik hujumlarni amalga oshirish yoki terroristik maqsadlarni targ'ib qilish uchun foydalanishni anglatadi. Bu hujumlar turli shakllarda bo'lishi mumkin, masalan, tashviqot tarqatish, ma'lumotlarni o'g'irlash yoki manipulyatsiya qilish yoki muhim infratuzilmani buzish. Shuningdek, buni kompyuterlar, tarmoqlar va ular saqlagan va tarqatgan ma'lumotlarga qarshi ruxsatsiz hujumlar va tahdidlar qilish harakati deb ham atash mumkin.[1]

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va jamiyat hayotining raqamlashtirilishi natijasida kiberxavfsizlik global xavfsizlikning muhim tarkibiy qismiga aylandi. Internet va raqamli infratuzilmaning keng qo‘llanilishi bilan bir qatorda, kiberterrorizm ham davlatlar, xalqaro tashkilotlar va jamiyat barqarorligiga jiddiy tahdid soluvchi omillardan biri sifatida namoyon bo‘lmoqda. Kiberterrorizm – bu axborot tizimlari, tarmoqlar va muhim infratuzilmalarni nishonga olib, siyosiy, mafkuraviy yoki iqtisodiy maqsadlarga erishish uchun amalga oshiriladigan zararli kiberhujumlar majmuasidir.[2]

So‘nggi yillarda kiberhujumlar soni va ko‘lami keskin ortib bormoqda. Biroq, barcha yirik kiberhujumlar ham kiberterrorizm sifatida tasniflanmaydi. Masalan, 2017-yilda sodir bo‘lgan WannaCry ransomware hujumi dunyo bo‘yicha 150 dan ortiq davlatdagi taxminan 200 mingdan ortiq kompyuter tizimlarini zararlagan va ko‘plab tashkilotlar faoliyatini izdan chiqargan. Ushbu hujum Buyuk Britaniyaning Milliy sog‘liqni saqlash tizimi faoliyatiga ham salbiy ta’sir ko‘rsatgan. Shunga qaramay, mazkur hujumning asosiy maqsadi moliyaviy foyda olish bo‘lgani sababli u kiberjinoyatchilik doirasiga kiradi.Xuddi shuningdek, NotPetya kiberhujumi global iqtisodiyotga katta zarar yetkazgan bo‘lib, uning zarari milliardlab AQSh dollariga baholangan. Ushbu hodisa ko‘proq davlatlararo ziddiyatlar kontekstida kiberurush elementi sifatida baholanadi.[3]2015-yilda Ukrainada elektr energiyasi tizimiga qilingan kiberhujum esa muhim infratuzilmaga qarshi amalga oshirilgan bo‘lib, aholining katta qismi vaqtincha elektrsiz qolishiga sabab bo‘lgan. (2-rasm) Bu kabi hujumlar, agar siyosiy yoki mafkuraviy maqsadlarda aholi orasida qo‘rquv uyg‘otishga qaratilgan bo‘lsa, kiberterrorizmga yaqinlashishi mumkin.[4]Shu sababli, kiberterrorizmni aniqlashda hujumning texnik ko‘lami emas, balki uning maqsadi va ijtimoiy-siyosiy ta’siri asosiy mezon hisoblanadi

Yirik davlat tashkilotlari ham kiberhujumlardan to‘liq himoyalangan emas. 2020-yilda aniqlangan SolarWinds ta’minot zanjiri hujumi natijasida AQSh hukumatining bir qator federal agentliklari hamda minglab tashkilotlar zarar ko‘rgan. Ushbu hodisa asosan kiberjosuslik yoki kiberurush elementi sifatida baholansa-da, u kiberhujumlarning milliy chegaralardan tashqarida sodir bo‘lishi va bir vaqtning o‘zida ko‘plab davlatlar manfaatlariga ta’sir ko‘rsatishi mumkinligini yaqqol namoyon etdi.Shu bilan birga, statistik ma’lumotlarga ko‘ra, ransomware turidagi kiberhujumlar soni ham keskin oshib bormoqda. 2023-yilda dunyo bo‘yicha 4591 ta ransomware hujumi qayd etilgan bo‘lsa, 2024-yilda bu ko‘rsatkich 5289 taga yetgan. Bu esa kiberjinoyatlar tobora murakkablashib borayotganini ko‘rsatadi.[5]

---

[1] Teohari va Rollins (2015).Theohary CA, Rollins JW. Kiberurush va kiberterrorizm: qisqacha. Kongress tadqiqot xizmati; Vashington, Kolumbiya okrugi: 2015. 2-bet.

[2] FBI. (2002). Cyber Terrorism: Testimony before the special oversight panel on terrorism. Federal Bureau of investigation.

[3]NotPetya ransomware attack on Maersk: key learnings. *LRQA*. Available at: https://www.lrqa.com/en/insights/articles/notpetya-ransomware-attack-on-maersk-key-learnings/

[4]Cyber- Attack Against Ukrainian Critical Infrastructure. *Cybersecurity and Infrastructure Security Agency (CISA)*. Available at: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

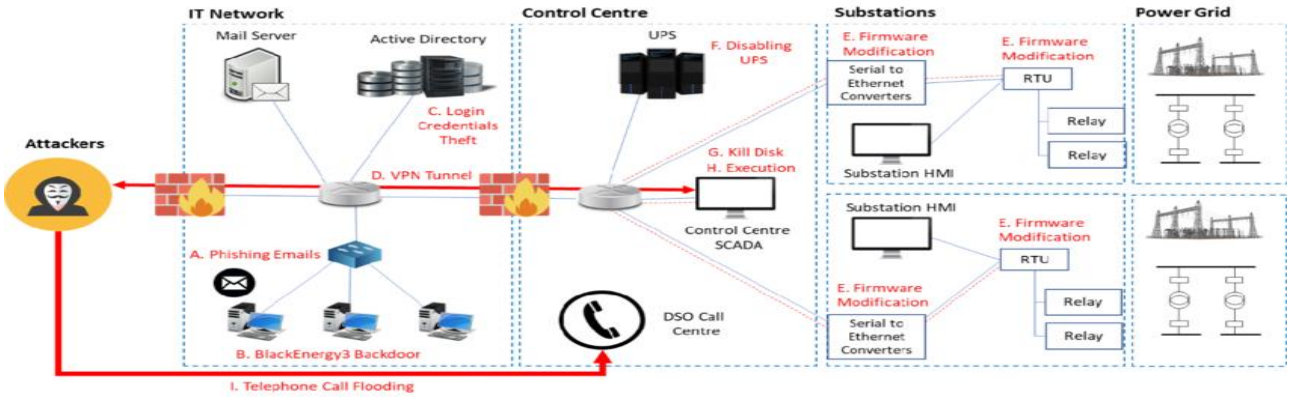
[5]Worldwide Ransomware Report 2024.U.S. Office of the Director of National Intelligence (ODNI) – Cyber Threat Intelligence Integration Center (CTIIC). Available at: https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf

Mazkur tendensiyalar fonida kiberterrorizm tahdidi ham dolzarb ahamiyat kasb etmoqda. Xususan, terroristik guruhlar raqamli texnologiyalardan nafaqat targ'ibot, balki bevosita hujum vositasi sifatida ham foydalanishga intilmoqda. Masalan, 2015-yilda "Cyber Caliphate" nomi bilan tanilgan guruh tomonidan Fransiyaning TV5Monde telekanaliga uyushtirilgan kiberhujum natijasida kanal efiri vaqtincha to'xtatilgan va uning axborot platformalarida ekstremistik mazmundagi materiallar joylashtirilgan.[6] Ushbu hodisa axborot makoniga qaratilgan kiberterrorizmning yorqin namunasi sifatida baholanadi.Bundan tashqari, ISHID tomonidan internet va ijtioiy tarmoqlar orqali olib borilgan keng ko'lamli kiberfaoliyatlar ham kiberterrorizmning zamonaviy shakllaridan biri hisoblanadi. Ushbu faoliyat yoshlarni radikallashtirish, qo'rquv muhitini shakllantirish va mafkuraviy ta'sir o'tkazishga qaratilgan bo'lib, global xavfsizlikka jiddiy tahdid tug'diradi.[7]

Shu sababli, kiberterrorizmni boshqa turdagi kiberhujumlardan ajratib ko'rish muhim ahamiyatga ega. Biroq, yuqorida keltirilgan barcha hodisalar umumiy kiberxavfsizlik muhitining murakkablashib borayotganini ko'rsatadi va bu esa terroristik guruhlar tomonidan ilg'or texnologiyalardan foydalanish ehtimolini yanada oshiradi. Natijada, kiberterrorizmga qarshi samarali kurashish uchun davlatlar o'rtasida hamkorlikni kuchaytirish hamda xalqaro mexanizmlarni rivojlantirish zarurati yanada ortib bormoqda.Bu esa kiberjinoyatlar tobora murakkablashib borayotganini va ularga qarshi kurashishda davlatlararo hamkorlik muhim ahamiyat kasb etayotganini ko'rsatadi.

Kiberterrorizmning asosiy xususiyatlaridan biri shundaki, u ko'pincha transmilliy xarakterga ega bo'lib, hujumchilar bir davlat hududida joylashgan bo'lsa-da, hujum boshqa davlat infratuzilmasiga qaratilishi mumkin. Shu sababli bunday jinoyatlarga qarshi samarali kurashish faqat milliy darajadagi choralar bilan cheklanib qolmay, balki xalqaro huquqiy hamkorlik mexanizmlarini rivojlantirishni ham talab qiladi.

1-rasm. 2015-yilda Ukrainadagi elektr energiyasi ta'minoti tizimiga kiberhujum natijasida 230 mingga yaqin iste'molchining bir necha soat davomida elektrsiz qolishi (manba: CISA, 2015)



Davlatlar o'rtasida axborot almashish, ekstraditsiya, qo'shma tergovlar hamda xalqaro konvensiyalar doirasida hamkorlik qilish kiberterrorizmga qarshi kurashning muhim vositalaridan hisoblanadi.

[6]BBC News. How France's TV5 was almost destroyed by 'Russian hackers'. Available at: https://www.bbc.com/news/technology-37590375

[7]Weimann, G. (2015). Terrorism in Cyberspace: The Next Generation. Washington, D.C.: Woodrow Wilson Center Press.

Shu munosabat bilan, kiberterrorizmga qarshi kurashishda xalqaro huquqiy hamkorlik mexanizmlarini o‘rganish, mavjud xalqaro normalar va institutlarning samaradorligini tahlil qilish hamda ularni takomillashtirish masalalari dolzarb ilmiy muammolardan biri hisoblanadi. Ushbu tadqiqot aynan kiberterrorizmga qarshi kurashda xalqaro huquqiy hamkorlik mexanizmlarining ahamiyatini tahlil qilishga va ularning samaradorligini oshirish bo‘yicha ilmiy xulosalar ishlab chiqishga qaratilgan.

METODLAR

Avvalo, tadqiqotning nazariy asosini shakllantirish maqsadida ilmiy adabiyotlar, xalqaro huquqiy hujjatlar va xalqaro tashkilotlar tomonidan e’lon qilingan rasmiy ma’lumotlar tahlil qilindi. Xususan, kiberjinoyatlar va kiberterrorizmga qarshi kurashish sohasidagi eng muhim xalqaro huquqiy hujjatlardan biri hisoblangan Budapest Convention on Cybercrime normalari o‘rganildi. Ushbu konvensiya kiberjinoyatlar bilan bog‘liq jinoyat tarkiblarini belgilash, davlatlar o‘rtasida huquqiy yordam ko‘rsatish hamda kiberjinoyatlar bo‘yicha xalqaro hamkorlikni rivojlantirish mexanizmlarini nazarda tutadi. Konvensiya kompyuter tizimlariga noqonuniy kirish, ma’lumotlarni buzish, kompyuter firibgarligi va boshqa kiberjinoyatlarni jinoyat deb e’tirof etishning yagona standartlarini belgilaydi.[8]Hozirga qadar **O‘zbekiston rasmiy ravishda Budapesht konvensiyasiga qo‘shilmagan**, ammo mamlakatda kiberxavfsizlikni mustahkamlash va xalqaro standartlarga moslash bo‘yicha ishlar olib borilmoqda. Shu sababli, kiberjinoyatlar va kiberterrorizmga qarshi samarali kurashish uchun O‘zbekistonning xalqaro mexanizmlar bilan integratsiyasi kelajakda muhim ahamiyat kasb etishi mumkin.

Tadqiqot jarayonida shuningdek xalqaro tashkilotlarning kiberxavfsizlik bo‘yicha strategiyalari ham tahlil qilindi. Jumladan, United Nations tomonidan ishlab chiqilgan xalqaro axborot xavfsizligi bo‘yicha hujjatlar, rezolyutsiyalar va tashabbuslar o‘rganildi. BMT doirasida davlatlar o‘rtasida kiberxavfsizlikni ta’minlash, kiberjinoyatlar bilan bog‘liq axborot almashish hamda xalqaro huquqiy mexanizmlarni rivojlantirishga qaratilgan bir qator tashabbuslar ilgari surilgan. Ushbu hujjatlar davlatlar o‘rtasida kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlikni mustahkamlashga xizmat qiladi.[9]

Tadqiqotda qiyosiy-huquqiy tahlil metodidan ham foydalanildi. Ushbu metod orqali turli davlatlar va xalqaro tashkilotlarning kiberterrorizmga qarshi kurashish borasidagi yondashuvlari solishtirildi. Jumladan, INTERPOL hamda Europol tashkilotlarining kiberjinoyatlarga qarshi kurashish mexanizmlari o‘rganildi. INTERPOL global miqyosda kiberjinoyatlar bo‘yicha axborot almashish tizimini yaratgan bo‘lib, u davlatlarning huquqni muhofaza qiluvchi organlari o‘rtasida tezkor hamkorlikni ta’minlaydi.[10] Europol esa Yevropa hududida kiberjinoyatlarga qarshi kurashish bo‘yicha maxsus markaz – European Cybercrime Centre (EC3) orqali xalqaro tergovlarni muvofiqlashtiradi.[11] Bundan tashqari, tadqiqot jarayonida tizimli tahlil metodidan foydalanildi. Ushbu metod yordamida kiberterrorizmga qarshi kurashishning xalqaro tizimi kompleks tarzda o‘rganildi. Xususan, kiberxavfsizlik sohasida faoliyat yuritayotgan North Atlantic Treaty Organization tashkilotining kiberxavfsizlik strategiyasi tahlil qilindi. NATO kiberhujumlarni zamonaviy xavfsizlik tahdidlaridan biri sifatida baholaydi va a’zo davlatlar o‘rtasida axborot almashish, qo‘shma

[8]Budapest Convention on Cybercrime.Council of Europe. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[9]ICT Security.United Nations Office for Disarmament Affairs. Available at: https://www.un.org/disarmament/ict-security/

[10]Cybercrime. INTERPOL. Available at: https://www.interpol.int/en/Crimes/Cybercrime

[11]Cybercrime – Europol. Europol. Available at: https://www.europol.europa.eu/crime-areas/cybercrime

mashg'ulotlar o'tkazish hamda kiberhujumlarga qarshi tezkor javob choralarini ishlab chiqish orqali kiberxavfsizlikni mustahkamlashga xizmat qiladi.[12]

Empirik tahlil metodidan foydalanib so'nggi yillarda sodir bo'lgan yirik kiberhujumlar misolida kiberxavfning amaliy oqibatlari o'rganildi. Shu bilan birga, mazkur tadqiqotda kiberterrorizm bilan kiberjinoyatchilik va kiberurush farqlari alohida e'tiborga olindi. Masalan, WannaCry ransomware attack, Yahoo va OPM ma'lumotlar buzilishi hamda SolarWinds supply chain attack kabi hodisalar asosan moliyaviy yoki kiberurush motivlariga ega bo'lgankiberhujumlar sifatida baholanishi mumkin, ular to'g'ridan-to'g'ri kiberterrorizm hisoblanmaydi.Shunga qaramay, ushbu hodisalar kiberhujumlarning **t**ransmilliy xususiyatga ega ekanligini va milliy chegaralardan oshib, bir vaqtning o'zida bir nechta davlat va tashkilotlarga ta'sir ko'rsatishi mumkinligini ko'rsatadi. Bu esa kiberterrorizm va kiberxavflarga qarshi samarali kurashishda xalqaro hamkorlik mexanizmlarining muhimligini yanada yaqqol ochib beradi.[13]

NATIJALAR

Olib borilgan tadqiqot natijasida kiberterrorizmga qarshi kurashishda xalqaro huquqiy hamkorlik mexanizmlarining samaradorligi va ularning amaliy qo'llanilish darajasi tahlil qilindi. Tadqiqot jarayonida xalqaro huquqiy hujjatlar, xalqaro tashkilotlar faoliyati hamda so'nggi yillarda sodir bo'lgan yirik kiberhujumlar misolida mavjud mexanizmlarning samaradorligi baholandi. Tahlil natijalariga ko'ra, kiberterrorizmga qarshi kurashishda eng muhim xalqaro huquqiy instrumentlardan biri Budapest Convention on Cybercrime ekanligi aniqlandi. Mazkur konvensiya davlatlar o'rtasida kiberjinoyatlarni jinoyat deb e'tirof etish, elektron dalillarni to'plash hamda huquqiy yordam ko'rsatish bo'yicha yagona standartlarni belgilab beradi. Tadqiqot natijalariga ko'ra, konvensiyaga qo'shilgan davlatlarda kiberjinoyatlarga qarshi qonunchilik bazasi sezilarli darajada takomillashtirilgani kuzatildi. Shuningdek, tadqiqot natijalari xalqaro tashkilotlar tomonidan yaratilgan hamkorlik mexanizmlari kiberjinoyatlar bilan kurashishda muhim rol o'ynashini ko'rsatdi. Xususan, INTERPOL tomonidan tashkil etilgan global axborot almashish tizimi davlatlarning huquqni muhofaza qiluvchi organlari o'rtasida tezkor hamkorlikni ta'minlaydi. Bu esa kiberjinoyatchilarni aniqlash va ularni javobgarlikka tortish jarayonining samaradorligini oshiradi. Tadqiqot davomida yirik kiberhujumlar ham tahlil qilindi. Jumladan, WannaCry ransomware attack natijasida 2017-yilda 150 dan ortiq davlatdagi 200 mingdan ortiq kompyuter tizimlari zararlangan. Ushbu hodisa kiberxavfsizlik tahdidlarining global xarakterga ega ekanligini va ularni bartaraf etishda xalqaro hamkorlik zarurligini ko'rsatdi.

Demak, tadqiqot natijalari shuni ko'rsatdiki, kiberterrorizmga qarshi kurashishda xalqaro huquqiy hamkorlikning asosiy samarali mexanizmlari quyidagilardan iborat:

- xalqaro konvensiyalar orqali yagona huquqiy standartlarni shakllantirish;
- davlatlar o'rtasida tezkor axborot almashish tizimlarini rivojlantirish;
- qo'shma tergovlar va operatsiyalarni amalga oshirish;
- xalqaro tashkilotlar orqali kiberxavfsizlik bo'yicha institutsional hamkorlikni kuchaytirish.

Natijalar shuni ko'rsatadiki, kiberterrorizmga qarshi kurashishda mavjud xalqaro huquqiy mexanizmlar muhim ahamiyatga ega bo'lsada, kiberjinoyatlarning tez rivojlanayotgan texnologiyalar bilan bog'liqligi sababli ushbu mexanizmlarni doimiy ravishda takomillashtirib borish zarur.

---

[12]Cyber Defence. NATO. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm

[13]Cybersecurity Advisories. Cybersecurity and Infrastructure Security Agency (CISA). Available at: https://www.cisa.gov/news-events/cybersecurity-advisories

MUHOKAMA

Tadqiqot natijalari shuni ko‘rsatadiki, kiberterrorizmning transmilliy xususiyati va tezkor rivojlanayotgan tabiati uni milliy choralar bilan cheklashning yetarli emasligini ko‘rsatadi.Davlatlar axborot almashish bo‘yicha bitimlar tuzdi, kiber tahdidlarni erta aniqlash tarmoqlari yo‘lga qo‘yildi. Endilikda jang maydoni — internet, qurol esa — kod. Bu kodlar o‘qdan ham tez, bombadan ham kengroq zarar yetkazishi mumkin. Ular devorlarni emas, tizimlarni buzadi; binolarni emas, axborotni yo‘q qiladi. Bugungi kunda kiber urushlar qurolli to‘qnashuvlar bilan teng xavf tug‘diradi. Ular iqtisodiy tizimlarni falaj qiladi, davlatlar orasida ishonchsizlik urug‘ini sochadi, hatto xalqaro siyosiy barqarorlikni izdan chiqaradi. Shuning uchun ham XXI asrda kiber makon insoniyat uchun yangi front chizig‘iga aylangan. Bu frontda jangchilar qo‘liga qurol emas, klaviatura olgan, ammo ularning har bir tugmani bosishi orqasida butun millat taqdiri turgan bo‘lishi mumkin.[14] Xalqaro hamkorlik mexanizmlari kiberterrorizmlarga va kiberhujumlarga qarshi samarali kurashishda muhim vosita bo‘lib xizmat qiladi. Xalqaro konvensiyalar, maxsus agentliklar va tashkilotlar orqali yaratilgan tizimlar nafaqat kiberjinoyatchilarni aniqlash va javobgarlikka tortish imkonini beradi, balki davlatlar infratuzilmalarini himoya qilishga ham xizmat qiladi. Misol uchun, Xitoy o‘z kiberxavfsizlik siyosatini milliy darajada kuchaytirish uchun bir qator huquqiy va texnik choralarni qo‘lladi. 2017-yilda kuchga kirgan Xitoy Kiberxavfsizlik to‘g‘risidagi Qonuni mamlakatning federal infratuzilmasini va aholining maxfiy ma’lumotlarini himoya qilishga yo‘naltirilgan (Yagya va Ashurova, 2023).[15] Shu bilan birga, Xitoyda kiberfavqulodda vaziyatlarga javob berish va kiberxavfsizlik siyosatini muvofiqlashtirish uchun tashkil etilgan CNCERT va Xitoy Kibermakon Ma'muriyati kabi agentliklar faoliyat yuritadi. Bu amaliyotlar Xitoyning kiberhujumlarga qarshi tezkor va koordinatsiyalangan javob berish qobiliyatini oshiradi.

Qo‘shma Shtatlar ham kiberterrorizmga qarshi kurashish bo‘yicha murakkab agentlik tizimiga ega. DHS muhim infratuzilmani himoya qilish va kiberhujumlarga qarshi choralarni muvofiqlashtirish bo‘yicha asosiy vazifani bajaradi, NCCIC esa axborot almashish va hodisalarga tezkor javob berishni ta’minlaydi. Shuningdek, FBI kiberjinoyatlarni tergov qiladi, DOD esa harbiy infratuzilmani himoya qiladi (Qi, Shao & Zheng, 2018;[16] Cunningham, 2021;[17]) Bu tizimlar milliy va xalqaro hamkorlikni mustahkamlash orqali kiberhujumlarni aniqlash va kamaytirishga imkon beradi.

Rossiya, Saudiya Arabistoni, BAA va Eronda ham kiberxavfsizlikni ta’minlash bo‘yicha maxsus agentliklar va qonunchilik mexanizmlari ishlab chiqilgan (Fischer, 2017;[18] Hindocha, 2020;[19]). Ushbu agentliklar kiberjinoyatchilarni aniqlash, huquqiy choralarni qo‘llash, muhim infratuzilmani himoya qilish va kiberhujumlarga qarshi profilaktik choralarni amalga oshirish bo‘yicha faoliyat yuritadi. Tadqiqot shuni ko‘rsatdiki, milliy siyosatning kuchli va samarali

---

[14]Sanger, D. E.,& Broad, W. J. (2012). “U.S. and Israel Said to Have Developed Computer Virus to Slow Iranian Nuclear Effort.” The New York Times.

[15] Yagya va Ashurova (2023).Yagya T, Ashurova Y. Shanxay Hamkorlik Tashkilotida Rossiya va Xitoy o'rtasidagi hamkorlikning rivojlanishi. Xalqaro siyosiy geografiyaning dolzarb masalalari materiallari; Cham. 2023. 77–85-betlar.

[16] Qi, Shao va Zheng (2018).Qi A, Shao G, Zheng W. Xitoyning kiberxavfsizlik qonunini baholash. Kompyuter qonunchiligi va xavfsizlik sharhi. 2018;34(6):1342–1354. doi: 10.1016/j.clsr.2018.08.007.

[17] Kanningem (2021).Kanningem H. Doktorlik dissertatsiyasi. 2021. Keng ko'lamli kiberterrorizm hujumining oldini olish va unga javob berishni yaxshilash.

[18] Fisher (2017).Fischer E. Kiberxavfsizlik muammolari va qiyinchiliklari. Kongress kutubxonasi; Vashington, Kolumbiya okrugi: 2017.

[19] Hindocha (2020).Hindocha A. AQShni tushunish bo'yicha o'quvchi qo'llanmasi. Kiberhujumlarni amalga oshirish arxitekturasi va byudjeti. Uchinchi yo'l. 2020. http://www.jstor.org/stable/resrep25036 . (2023-yil 18-iyun). http://www.jstor.org/stable/resrep25036 [Ma'lumotnomalar ro'yxati]

mexanizmlari global hamkorlikni qo'llab-quvvatlaydi va kiberterroristik tahdidlarning oqibatlarini sezilarli darajada kamaytiradi.

Albatta kiberterrorizm muammosi nafaqat xorijda balki bizning davlatimizda ham kiberhuquq sohasidagi asosiy pozitsiyasiga ega bo'lib bormoqda. salasi bugun har qachongidan ham dolzarb ahamiyat kasb etmoqda.Kiberterrorizmning xavflilik darajasini O'zbekiston Respublikasi Prezidenti Sh.Mirziyoyev shunday ta'kidlaydi, "…bugun dunyoning deyarli barcha mamlakatlari kibermakondagi terrorizm bilan to'qnashmoqda. Internet radikal g'oyalarni tarqatish, odamlarni yollash, terrorchilik harakatlarini moliyaviy ta'minlash, rejalashtirish va sodir etish vositasiga aylanmoqda". Shu boisdan bugungi kunda kiberjinoyatlarni paydo bo'lishining nazariy asoslari, kiber jinoyat va kiberterrorizmning huquqiy tushunchalarini ishlab chiqish, kiberterrorizmga qarshi kurashda xalqaro va mintaqaviy tashkilotlarda takomillashtirish, kiberterrorizm qarshi kurashda davlatlar hamkorligini rivojlantirish o'z navbatida mazkur muammo doirasida ilmiy tadqiqotlarning ustuvor amalga oshirilishini talab etmoqda.[20]Bu esa shubxasiz mustahkam himoya va kibermakonda hushyorlikni oshirishga omil bo'lib xizmat qiladi. Aynan shunday xavflarni oldini olsih maqsadida O'zbekiston hukumati kiberterroristik tahdidlarga qarshi kurashda milliy qonunchilik va institutlarni rivojlantirdi. Xususan "Shaxsga doir ma'lumotlar to'g'risida"gi qonuni qabul qilindi, bu davlat va xususiy infratuzilmalarni himoya qilish, shaxsiy ma'lumotlarni noqonuniy foydalanishdan saqlashga qaratilgan. Bundan tashqari O'zbekiston Respublikasi prezidedntining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida" PQ-4452 son qarori – axborot-kommunikatsiya tizimlarini himoya qilish va kiberterroristik hujumlarni aniqlash uchun chora-tadbirlar, shu asosda "Kiberxavfsizlik markazi" tashkil etilgan. Va ushbu sohada tayanch hujjat bo'lib "Kiberxavfsizlik to'g'risida"gi qonun xizmat qilmoqda. Bu milliy kiberinfratuzilmalarni, davlat va xususiy sektor resurslarini kiberterrorizm tahdidlariga qarshi mustahkamlashni belgilaydi.

Muhokama davomida shuni aniqlash mumkinki, kiberterrorizmning rivojlanayotgan tabiati yangi tahdidlar va innovatsion hujum vektorlari bilan bog'liq. Kiberterroristik guruhlar sanoat nazorati tizimlari (ICS) va IoT qurilmalariga hujumlar, ilg'or doimiy tahdidlar (APT) va ma'lumotlarni manipulyatsiya qilish kabi taktikalarni qo'llamoqda. Shuningdek, kiberterrorizm global xarakterga ega bo'lib, guruhlar dunyoning istalgan nuqtasidan hujumlar uyushtirishi mumkin. Bu esa davlatlar va xalqaro tashkilotlar uchun kiberhujumlarga tezkor va moslashuvchan javob strategiyalarini ishlab chiqishni zarur qiladi.

Natijalar shuni ko'rsatadiki, kiberterrorizmga qarshi samarali kurashish uchun quyidagi yo'nalishlar muhim:

- Xalqaro konvensiyalarni kengaytirish va kiberjinoyatlarning yangi turlarini qamrab olish;
- Milliy va xalqaro axborot almashish tizimlarini rivojlantirish;
- Qo'shma tergovlar va kiberoperatsiyalarni muvofiqlashtirish;
- Xalqaro tashkilotlar orqali institutsional hamkorlikni kuchaytirish va doimiy malaka oshirish dasturlarini joriy etish;
- Kiberxavfsizlik tadqiqotlari va texnologik yangilanishlarga sarmoya kiritish;
- Jamoatchilik xabardorligi va tayyorgarligini oshirish orqali potentsial oqibatlarni kamaytirish.

[20]S.Xasanova. "KIBERTERRORIZMGA QARSHI KURASHDA XALQARO-HUQUQIY HAMKORLIK: GLOBAL TAHDIDLARGA BIRLASHGAN JAVOB" – Toshkent.; - 2020

Shu bilan birga, tadqiqot shuni ko'rsatdiki, texnologiyalarning tez rivojlanishi, 5G, kvant hisoblash va sun'iy intellekt kabi innovatsiyalar kiberhujumlarni aniqlash va oldini olish jarayonini yanada murakkablashtirmoqda. Shu sababli, kiberxavfsizlik choralarini yangilash va doimiy nazorat mexanizmlarini takomillashtirish kiberterroristik tahdidlarga qarshi samarali kurashning ajralmas qismi hisoblanadi. Natijada, global siyosat, milliy qonunchilik va xalqaro hamkorlik mexanizmlari birgalikda kiberterroristik tahdidlarga qarshi javob berish va muhim infratuzilmalarni himoya qilishda asosiy vosita sifatida xizmat qilmoqda.

XULOSA

Kiberterrorizm internet va boshqa kompyuter texnologiyalaridan foydalanib, moliyaviy, siyosiy va ijtimoiy jarayonlarga zarar yetkazuvchi jiddiy global tahdid bo'lib qolmoqda. Bu kabi hujumlar nafaqat moliyaviy yo'qotishlarga, balki obro'ga zarar yetkazishga va jamiyat barqarorligiga xavf tug'diradi.

Shuningdek, kiberxavfsizlikni oshirish va muhim tizimlarning chidamliligini kuchaytirish bo'yicha global sa'y-harakatlar amalga oshirilmoqda. Bu sa'y-harakatlar texnik choralarni (xavfsizlik devorlari, antivirus dasturlari) va texnik bo'lmagan choralarni (xodimlarni o'qitish, hodisalarga javob berish rejalari) o'z ichiga oladi. Shu bilan birga, kiberterroristik tahdidlar tez rivojlanayotganligi va internetning o'zgaruvchan tabiati ushbu sa'y-harakatlarning doimiy yangilanishini talab qiladi. Olingan natijalar shuni ko'rsatadiki, shaxslar va tashkilotlar kiberxavfsizlik choralarini muntazam yangilab, xavfsizlik protokollariga rioya qilish orqali kiberterrorizm tahdidini kamaytirishlari mumkin. Shu bilan birga, kiberhujumlarning turli shakllari va sohalarga ta'siri tufayli, hukumatlar va biznes uchun strategik va ishonchli kiberxavfsizlik siyosatlarini ishlab chiqish muhim ahamiyatga ega. Kelajakdagi tadqiqotlar uchun tavsiya qilinadi, kiberterrorizmga qarshi kurashishning samaradorligini o'lchash va mamlakatlar tomonidan ishlab chiqilgan siyosatlarning haqiqiy ta'sirini baholashga qaratilgan tadqiqotlar olib borilishi kerak.

Foydalanilgan manbalar:

1. Abdixakimov, I. B. (2025). *Kiber huquq [Matn]: o'quv qo'llanma*. Toshkent: TDYU nashriyoti.
2. Qi, A., Shao, G., & Zheng, W. (2018). Evaluating China's cybersecurity law. *Computer Law & Security Review, 34*(6), 1342–1354. https://doi.org/10.1016/j.clsr.2018.08.007
3. Kanningem, H. (2021). *Preventing and responding to large-scale cyberterrorism attacks* [Doctoral dissertation].
4. Fischer, E. (2017). *Cybersecurity issues and challenges*. Library of Congress; Washington, DC.
5. Hindocha, A. (2020). *Understanding the U.S.: Cyberattack execution architecture and budgeting*. Third Way. Retrieved June 18, 2023, from http://www.jstor.org/stable/resrep25036
6. Yagya, T., & Ashurova, Y. (2023). Development of cooperation between Russia and China within the Shanghai Cooperation Organization. *Materials on Current Issues of International Political Geography*, Cham, 77–85.
7. Theohary, C. A., & Rollins, J. W. (2015). *Cyberwar and cyberterrorism: An overview*. Congressional Research Service; Washington, DC.
8. Federal Bureau of Investigation. (2002). *Cyber terrorism: Testimony before the special oversight panel on terrorism*.
9. UK Parliament Research Briefings. Retrieved from https://researchbriefings.files.parliament.uk/
10. United Nations. Retrieved from https://www.un.org/
11. U.S. Department of Homeland Security. Retrieved from https://www.dhs.gov/

12. Cybersecurity & Infrastructure Security Agency (CISA). Retrieved from https://www.cisa.gov/
13. Office of the Director of National Intelligence. Retrieved from https://www.dni.gov/
14. North Atlantic Treaty Organization (NATO). Retrieved from https://www.nato.int/