ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

KIBERTERRORIZM VA XALQARO HUQUQIY BAZALAR.

Abdusattorov Shaxzod
Toshkent davlat yuridik universiteti magistraturasi talabasi

ANNOTATSIYA

So’nggi yillarda xalqaro kiberterrorizmning kuchayishi butun dunyo bo’ylab qo’rquv, halokat va buzilishlarni keltirib chiqaradigan kompyuterga asoslangan jinoiy faoliyatga olib keldi. Kiberterrorizmga qaratilgan milliy qonunlar va siyosatlar asosan rivojlangan davlatlar bilan cheklangan va 21-asr kiberterrorizmini yaxlit boshqara olmaydi. Kiberterrorizmga qarshi kurash bo‘yicha xalqaro huquqiy baza yo‘qligini hisobga olib, butun dunyo bo‘ylab rasmiylar va hukumatlar kiberterrorizm uchun mas’ul shaxslarni topish va jinoiy javobgarlikka tortishda o‘ta qiyinchiliklarga duch kelishmoqda.

Ushbu maqola yaxlit xalqaro huquqiy bazaning zarurligi haqida bahs yuritadi; samarali xalqaro huquqiy bazani yaratish uchun asosiy elementlarni ajratib ko’rsatadi; va amaldagi xalqaro shartnomalar va transchegaraviy bitimlarni belgilaydi, ularni jinoiy javobgarlikka tortish uchun qonunchilik qoidalarini taqdim etish uchun kengaytirilishi mumkin.

Kalit so’zlar: Kiberterrorizm, xalqaro huquqiy asoslar, ta’riflar, muammolar, Birlashgan Millatlar Tashkiloti, xalqaro shartnomalar, yurisdiktsiya, prokuratura.

АННОТАЦИЯ

В последние годы рост международного кибертерроризма привел к компьютерной преступной деятельности, вызывающей страх, разрушения и разрушения во всем мире. Национальные законы и политика по борьбе с кибертерроризмом в значительной степени ограничены развитыми странами и не могут комплексно бороться с кибертерроризмом 21 века. Учитывая отсутствие международно-правовой базы для борьбы с кибертерроризмом, власти и правительства во всем мире сталкиваются с огромными трудностями в поиске и привлечении к ответственности виновных в кибертерроризме.

В этой статье приводятся доводы в пользу необходимости последовательной международной правовой базы; освещаются основные

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

элементы создания эффективной международно-правовой базы; и определяет существующие международные договоры и трансграничные сделки, которые могут быть расширены, чтобы предусмотреть законодательные положения для их криминализации.

Ключевые слова: Кибертерроризм, международно-правовая база, определения, проблемы, Организация Объединенных Наций, международные соглашения, юрисдикция, судебное преследование.

ANNOTATION

In recent years, the rise of international cyber terrorism has led to computer-based criminal activity causing fear, destruction and disruption around the world. National laws and policies addressing cyberterrorism are largely limited to developed countries and cannot comprehensively manage 21st century cyberterrorism. Given the lack of an international legal framework to combat cyber-terrorism, authorities and governments around the world face extreme difficulties in finding and prosecuting those responsible for cyber-terrorism.

This article argues for the need for a coherent international legal framework; highlights the main elements for creating an effective international legal framework; and defines existing international treaties and cross-border transactions that can be extended to provide statutory provisions for criminalizing them.

Key words: Cyberterrorism, international legal framework, definitions, problems, United Nations, international agreements, jurisdiction, prosecution.

KIRISH

So’nggi yillarda kiberterrorizm va terrorchilik xurujini rejalashtirish va uyushtirishda aybdorlarni aniqlash va jinoiy javobgarlikka tortish bo’yicha qonunchilik va ta’sir choralarini qo’llash zaruratidan xavotir ortib bormoqda. Logistika nuqtai nazaridan, har qanday miqdordagi jinoyatchilar dunyo bo’ylab qayerda joylashganidan qat’i nazar manbalardan shu jumladan jismoniy shaxslardan, uyushgan jinoyatchilik sindikatlaridan va agentliklardan hujumlarni rejalashtirishi va amalga oshirishi mumkin. Hujumlar kompyuter tarmog’idan foydalanadigan har qanday ob’ektni nishonga olishi mumkin. Kiberterrorchilik faoliyati sonining ortib borayotgani raqamli asrda kiberterrorizm jinoyatchilarini topish va jinoiy javobgarlikka tortishda milliy davlatlar qanday qiyinchiliklarni boshdan kechirayotganini ko‘rsatadi.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

Kiberxavfsizlikda paydo bo'ladigan tahdidlar muammosiga xalqaro e'tibor kuchayib borayotganini ko'rish mumkin va yurisdiksiyaviy ta'qib qilish va transchegaraviy huquqni qo'llash choralarini ishlab chiqish uchun huquqiy baza zarur. Biroq, xalqaro hamjamiyat keng ko'lamli ko'rsatmalarni yaratgan bo'lsada, mavjud xalqaro konventsiyalar va qonunchilik kiberterrorizmni o'z ichiga olmaydi yoki samarali bo'lishi uchun yetarlicha uzoqni ko'ra olmaydi. Yaxlit xalqaro huquqiy bazaning yo'qligi sababli davlatlar kiberterrorizmga qarshi kurashish uchun o'zlarining ichki qonunlarini faol ravishda ishlab chiqishlari, amalga oshirishlari va qo'llashlariga olib keldi. Davlatlarga kiberterrorizm aybdorlarini topish va jinoiy javobgarlikka tortish uchun samarali huquqiy choralar ko'rish uchun xalqaro huquqiy bazani ishlab chiqish va yaratish uchun jiddiy xalqaro hamkorlik talab etiladi.

Kiberterrorimzda xalqaro qonunchilikning o'rni.

Kiberterrorchilar asosan kompyuterlar tomonidan boshqariladigan tizimlarni nishonga oladi. Ushbu tizimlar kommunal xizmatlar (suv, elektr va gaz ta'minoti), havo harakatini boshqarish tizimlari, bank va moliya, telekommunikatsiya va transport tizimlari kabi muhim infratuzilmani o'z ichiga olishi mumkin. Kiberterrorizm muhim infratuzilma uchun katta xavf tug'diradi. Avstraliyada hukumati muhim infratuzilmani quyidagicha belgilaydi:

"Agar vayron qilingan, buzilgan yoki uzoq vaqt davomida mavjud bo'lmasa, mamlakatning ijtimoiy yoki iqtisodiy farovonligiga sezilarli ta'sir ko'rsatadigan yoki Avstraliyaning milliy mudofaa va milliy xavfsizlikni ta'minlash qobiliyatiga ta'sir qiladigan jismoniy vositalar, ta'minot zanjirlari, axborot texnologiyalari va aloqa tarmoqlari".[1]

Kiberterrorizm inson salomatligi, yashashi uchun haqiqiy xavf tug'diradi, aholi, qo'shni davlatlar va dunyoning boshqa mamlakatlari uchun potentsial xavfli oqibatlarga olib kelishi mumkin edi. Tadqiqotlar shuni ko'rsatadiki, Stuxnet virusi AQSh, Indoneziya, Hindiston, Ozarbayjon, Pokiston va boshqalar kabi uzoq mamlakatlardagi kommunal xizmatlarni boshqaradigan kompyuter tarmoqlariga ham ta'sir qilgan. Shunday qilib, hukumatlar uning muhim infratuzilmasiga, jumladan,

[1] 2. Attorney-General's Department. (2010). Critical infrastructure resilience strategy. Canberra: Commonwealth Of Australia.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

harbiy va yadroviy inshootlarga kiberterror hujumi ob'ekti bo'lmasligiga katta e'tibor berishlari kerak.

Hukumatlarning bunday hujumlarning oldini olish va ularga qarshi kurashish qobiliyati bir qancha omillarga bog'liq

Tegishli qonunchilikning mavjudligi va amalga oshirilishi muhim ahamiyatga ega. Hozirgi vaqtda kiberterrorchilik xurujlari bo'yicha xalqaro tartibga solishning yo'qligi hisobga olinsa, har bir davlatga qonuniy choralar ko'rish uchun o'z ichki qonunlariga tayanishi kerak. Jinoyatchilarni bunday hujumlar uchun jinoiy javobgarlikka tortish jinoyatchi bir mamlakatda yashagan joyda muvaffaqiyatli bo'ladi. Avstraliyada kengashning sobiq xodimi 2001-yilda muhim infratuzilmani boshqaruvchi kengash kompyuterlariga buzib kirgani va ularni millionlab litr xom kanalizatsiyani umumiy suv yo'llariga quyish uchun dasturlashtirgani uchun ikki yilga qamalgan. Agar rasmiylar tajovuzkorning boshqa davlatda ekanligini aniqlasa, bu davlatning hamkorligi va o'zaro munosabati zarur va har doim ham bo'lishi mumkin emas. Bunday hollarda, hujumning oldini olish, shuningdek, hujum uchun javobgar shaxsni jinoiy javobgarlikka tortish uchun xalqaro tashkilotlar va boshqa davlatlarga tayanish talab qilinadi. 2007-yilda Estoniyada mamlakatning eng yirik banklari, gazetalari, maktablari va boshqa ko'plab muassasalarga ommaviy kiberhujumlar sodir bo'ldi natijada Estoniya "Yevropa Ittifoqi, NATO urushning yangi shakliga qat'iy javob berish" so'roviga sabab bo'ldi.

Hujum sodir etilgan mamlakatdan tashqarida yurisdiktsiyalarda faoliyat yuritayotgan kiberterrorchilarni jinoiy javobgarlikka tortishning murakkabligi yoki ba'zan qobiliyatsizligi xalqaro asosning yo'qligi bilan bog'liq muammolarni ko'rsatadi. Bunga qo'shimcha ravishda huquqiy tartib-qoidalar va tizimlar mamlakatdan mamlakatga farq qiladi va xalqaro sudlar amalda juda cheklangan vakolatlarga ega bo'lib, ijro etishni qiyinlashtiradi. Bu kiberterrorizmga oid xalqaro qonunlarning amaldagi cheklangan qo'llanilishini kengaytirish va samarali xalqaro huquqiy bazaga ehtiyojni kengaytirish haqidagi dalillarni qo'llab-quvvatlaydi.

SAMARALI XALQARO HUQUQIY NEZALARNI TASHLASH

Samarali xalqaro huquqiy bazani yaratish uchun to'rtta muhim element quyidagilardir: kiberterrorizmni aniqlash bo'yicha kelishuv; Birlashgan Millatlar Tashkiloti (BMT) tomonidan rahbarlik; yaxlit va mustahkam tizim yaratish uchun

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

amaldagi xalqaro konventsiyalar, qonunchilik va vakolatlardan foydalanish va kengaytirish; va samarali huquqni muhofaza qilish.

Kiberterrorizmning ta'riflari

Kiberterrorizmga qarshi kurash bo'yicha xalqaro huquqiy bazaning birinchi muhim elementi xalqaro kelishuv va kiberterrorizmga oid atamalarning ta'riflari to'plamini qabul qilishdir. Bugungi kunga qadar BMT xalqaro terrorizmga qarshi maxsus terrorchilik faoliyati bilan bog'liq bo'lgan o'n to'rtta konventsiya va to'rtta tuzatishni ishlab chiqdi (Birlashgan Millatlar Tashkiloti, n.d.). Biroq, ushbu Konventsiyalar doirasida terrorizmning aslida nima ekanligining umume'tirof etilgan ta'rifi haligacha mavjud emas. Buning o'rniga, a'zo davlatlardan Konventsiyalarga umumiy tarzda murojaat qilishlari va o'zlarining ta'riflarini ishlab lozim.

Xalqaro hamjamiyat 2010-yilda Birlashgan Millatlar Tashkilotining Terrorizmga qarshi kurash qo'mitasi Ijroiya boshqarmasi (CTED) tashkil etilishi bilan ushbu muammoni hal qila boshladi. Boshqarmaning vazifasi qonunchilikni ko'rib chiqish va kerakli hulosalar ishlab chiqish. Shunga qaramay, kiberterrorizm ta'rifi bo'yicha aniqlik yo'qligi ko'plab mamlakatlar tomonidan asosiy muammo sifatida tan olingan ko'pchilik ushbu muammoni mahalliy darajada hal qilish uchun o'z qonunchiligini ishlab chiqadi.

Islom Konferensiyasi Tashkilotining Xalqaro terrorizmga qarshi kurash to'g'risidagi konventsiyasining 1-moddasida terrorizmga quyidagicha ta'rif berilgan:

Har qanday zo'ravonlik harakati yoki tahdidi, uning maqsadi yoki niyatidan qat'i nazar, odamlarni qo'rqitish yoki ularga zarar etkazish yoki ularning hayoti, sha'ni, erkinliklari, xavfsizligi yoki huquqlariga tahdid solish yoki atrof-muhitni fosh qilish maqsadida individual yoki jamoaviy jinoiy rejani amalga oshirish uchun qilingan yoki har qanday ob'ekt yoki davlat yoki xususiy mulkni xavf ostiga qo'yish yoki ularni egallash yoki tortib olish, milliy resurs yoki xalqaro ob'ektlarni xavf ostiga qo'yish yoki mustaqil davlatlarning barqarorligi, hududiy yaxlitligi, siyosiy birligi yoki suverenitetiga tahdid solishi.

Biroq Konventsiyaning 2-moddasining "a" bandida "Xalqlarning xalqaro huquq tamoyillariga muvofiq ozodlik va o'z taqdirini o'zi belgilashga qaratilgan xorijiy bosqinchilik, bosqinchilik, mustamlakachilik va gegemonlikka qarshi qurolli kurashi terrorchilik jinoyati deb hisoblanmaydi. '. Misol uchun, agar biror mamlakatda kiberterrorchilik akti sodir etgan shaxslar Afg'onistonda joylashgan bo'lsa

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

(Konventsiyaga a'zo 57 davlatdan birida) ular o'zlarining terroristik harakati xorijiy ishg'olga qarshi kurash akti ekanligini da'vo qilishlari mumkin va shuning uchun bu ta'rifga kirmaydi.

Birlashgan Millatlar Tashkilotining rahbarligi

Birlashgan Millatlar Tashkiloti o'zgarishlar tayyor bo'lishi va a'zo davlatlarning yig'ilishlari va kelishuvga erishishi va kiberterrorizm bo'yicha umumiy tushunchaga ega bo'lishi uchun yordamchi bo'lishi kerak. Birlashgan Millatlar Tashkilotining Atom energiyasi bo'yicha Xalqaro agentlik kabi agentliklari hozirda unga a'zo davlatlar bilan kiberxavfsizlik hodisalarini ta'qib qilish uchun tegishli xalqaro huquqiy bazani yaratish maqsadida ishlamoqda.

Birlashgan Millatlar Tashkiloti CTEDdan a'zo davlatlarga ma'lumot almashish va terrorchilarga nisbatan yurisdiksiyaviy ta'qib qilish choralarining kengroq muhim masalalarini muhokama qilish imkoniyatlarini taqdim etish orqali kiberterrorizm sohasidagi jinoyatlarni boshqarish uchun turli ichki jinoiy qonunlarni uyg'unlashtirishda katta ro'l o'ynashda foydalanishi mumkin. 2010-yildan beri CTED "barcha 192 a'zo davlat bilan terrorizmni jinoiy javobgarlikka tortish, terrorchilarni javobgarlikka tortish, terrorchilarni moliyaviy qo'llab-quvvatlashning oldini olish va ularning xavfsiz boshpana topishlari va chegaralarni kesib o'tishlariga yo'l qo'ymaslik bo'yicha qanday choralar ko'rganligi to'g'risida dialog o'tkazdi". CTEDning vakolatlarini hozirgi rolidan tashqari kengaytirish a'zo davlatlar uchun standartlashtirilgan asosiy texnik shartlarni o'z ichiga olgan yagona qonunchilik bazasiga olib kelishi mumkinligi haqida bahslashish mumkin.

Birlashgan Millatlar Tashkiloti barcha a'zo davlatlarning (shu jumladan, rivojlanayotgan mamlakatlarning) ichki qonunchiligida kiberterrorizmni tergov qilish va ta'qib qilish uchun tegishli vakolatlarni ta'minlash bo'yicha kelishuvga erishish mumkin bo'lgan ideal forumdir. Ushbu xalqaro hamkorlik kiberrazvedka ma'lumotlarini almashish uchun tezkor, sezgir va samarali muvofiqlashtirish boshqaruv tizimini yaratish yo'lida faol ishlashi mumkin. Kiberhujumlarga tegishli, mutanosib va tejamkor bo'lgan har tomonlama javob berishni ta'minlash bo'yicha ko'rsatmalar bo'yicha qo'shma kelishuvga erishish mumkin.

Konventsiyalar, qonunlar va hokimiyatlar

Mamlakatlar tomonidan ratifikatsiya qilingan (va davom etayotgan) mavjud konventsiyalar va shartnomalar xalqaro hamkorlikka asoslanishi mumkin bo'lgan

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

mustahkam poydevor bo'lib xizmat qiladi. Garchi ular keng ko'rsatmalar to'plamini taqdim etsa-da, ular kiberterrorizmni o'z ichiga olishi yoki global kiberterrorizmga qarshi kurashish va unga qarshi kurashishda samarali bo'lishi uchun kengaytirilishi kerak (qonunchilik va mintaqaviy).

Samarali xalqaro huquqiy bazani yaratish uchun amaldagi shartnoma va konvensiyalarni kiberterrorizmga qarshi milliy qonunchilikni rivojlantirish imkonini beruvchi keng qamrovli yo'riqnomalarni o'z ichiga olgan holda kengaytirish kerak. Ushbu ko'rsatmalar, shuningdek, huquqni muhofaza qilish idoralari jinoyatchilarga qarshi kurashish uchun xalqaro resurslardan foydalanishi uchun o'zaro ma'lumot to'plash va almashishni o'z ichiga olishi va ruxsat berishi kerak.

Yevropa Kengashining Kiberjinoyatlar to'g'risidagi konventsiyasi

Yevropa Kengashining Kiberjinoyatlar to'g'risidagi konventsiyasi kiberjinoyatlar bo'yicha yagona majburiy xalqaro hujjatdir (Yevropa Kengashi, n.d.). Konventsiya kiberjinoyatchilikka qarshi keng qamrovli milliy qonunchilikni ishlab chiqish, shuningdek, ushbu shartnoma ishtirokchi-davlatlari o'rtasidagi xalqaro hamkorlik uchun umumiy asosni taqdim etadi. Ushbu Konventsiyani yanada samaraliroq qilish uchun u hozirgi dolzarbligi va Yevropada qo'llanilishi doirasidan tashqarida kengayishi kerak. Yana bir muhim omil shundaki, Konventsiya faqat "Internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlarga, xususan mualliflik huquqining buzilishi, kompyuter bilan bog'liq firibgarlik, bolalar pornografiyasi va tarmoq xavfsizligini buzish bilan bog'liq" (Kiber jinoyatlar to'g'risidagi konventsiya) va bunday emas. Xususan, kiberterrorizm kiradi. Samarali mexanizm bo'lishi uchun kiberterrorizmni kiritish kerak.

Ushbu Konventsiya rivojlanish salohiyatiga ega, 2012-yil sentabrida 37 ta davlat, shu jumladan AQSh, Yaponiya, Kanada va Janubiy Afrika Konventsiyani ratifikatsiya qilgan. Konventsiyani hali ratifikatsiya qilmagan o'nta davlat Konventsiyaning kiberterrorizmga qarshi kurash bo'yicha ichki qonunlar va tergov o'rtasidagi o'xshashlikni ishlab chiqish va joriy etish mexanizmi sifatida samaradorligiga to'sqinlik qilmoqda. Bu, o'z navbatida, xalqaro hamjamiyatning kiberterrorchilik hujumlarini jinoiy javobgarlikka tortish majburiyatini olishga qaratilgan sa'y-harakatlarga ta'sir qiladi. Shunga qaramay, 100 dan ortiq davlatlar konventsiyadan kiberjinoyat tahdidiga qarshi kurashish uchun asos sifatida foydalanib, o'zlarining ichki qonunchiligini mustahkamlamoqda.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

Shimoliy Atlantika Shartnomasi Tashkiloti

Shimoliy Atlantika Shartnomasi Tashkilotining (NATO) kiberterrorizmga qarshi kurash bo'yicha aniq majburiyati Kibermudofaa boshqaruvi boshqarmasi va Kooperativ Kibermudofaa Mukammallik Markazini tashkil etishdan iborat. NATO hozirda kiberhujumga qarshi tezkor harakat guruhini yaratmoqda va 2012-yil oxirida ishga tushishi kutilmoqda.

Samarali huquqni muhofaza qilish

Huquqni muhofaza qilish idoralari oldida kiberterrorizm bilan bog'liq muammolar ko'p. Kompyuter texnologiyalarining jadal rivojlanishi butun dunyo bo'ylab kiberterrorizmning chastotasi va ta'sirini oshirdi. Bu kiberterrorchilar yagona xalqaro qonunchilik yo'qligini bilgan holda chegarasiz muhitda o'z faoliyatini davom ettirmoqda. Hukumatlar kiberterroristik harakatlarga qarshi kurashish uchun turli xil texnik vakolatlarga ega va huquqni muhofaza qilish organlari o'rtasidagi muvofiqlashtirish tashqi siyosat va siyosiy mafkuralar bilan cheklangan. Dunyo bo'ylab huquqni muhofaza qilish idoralari ham moliyalashtirish va kiberterrorizm bo'yicha o'qitilgan xodimlar bilan bog'liq resurslar bilan cheklangan. Bu o'z navbatida kibertahdidlar haqidagi ma'lumotlarni huquqni muhofaza qiluvchi organlarga uzatish va almashishning xavfsiz mexanizmini ishlab chiqish masalasini ko'taradi. Mavjud xalqaro qonunchilik muhiti kiberterrorizmni sodir etgan jinoyatchilarni juda cheklangan yoki umuman to'xtatib turishini ta'kidlab o'tish mumkin.

Mamlakatlar kiberterrorizmga qarshi kurashish uchun hukumatlar, ularning huquqni muhofaza qilish idoralari va sanoat uchun siloslarda ishlashni to'xtatish juda muhimdir. Muvofiqlashtirilgan xalqaro harakatlar mamlakatlarga tobora kengroq miqyosda ta'sir o'tkazayotgan ushbu global muammoni hal qilishning yagona yo'lidir. Madaniy siljish barcha hukumatlar, axborot texnologiyalari, huquqni muhofaza qilish organlari va huquq sohalarida amalga oshirilishi kerak. Huquqni muhofaza qilish idoralari va sanoat axborot almashishni yaxshilash uchun hamkorlik qilishlari kerak, xususan, ularning yangi va paydo bo'lgan tahdidlarni, shu jumladan hujum usullarini aniqlash va ogohlantirishdagi tezkorligi. Advokatlar, sud tizimi va jamoatchilikni kiberterrorizm bo'yicha keng qamrovli ta'lim va xabardorlik dasturi ham kiberterrorizm bo'yicha jinoiy javobgarlikka tortilish ehtimolini oshirishga yordam berishi mumkin. Sanoat va huquq-tartibot idoralari ham huquqiy jarayon va dalillarni to'plash va sud jarayonida taqdim etishga qo'yiladigan talablar haqidagi

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

tushunchalarini oshirishi va yaxshilashi kerak. Bu aniqroq tizimlashtirilgan tergovlarni osonlashtiradi va sudlarga yanada ishonchli ma’lumotlar taqdim etilishiga olib keladi.

XULOSA

Mavjud xalqaro konventsiyalar va shartnomalar kiberterrorizmni ta’qib qilish va unga qarshi kurashishda samarali emasligi ko’rinib turibdi. Shunday qilib, kiberterrorizm keltirib chiqaradigan muammolarni hal qilish uchun yaxlit xalqaro huquqiy baza talab qilinadi. Samarali asos yaratish uchun mavjud shartnomalar va konventsiyalar kiberterrorizmga oid keng qamrovli ko’rsatmalarni o’z ichiga olgan holda kengaytirilishi kerak. Ushbu ko’rsatmalar, shuningdek, huquqni muhofaza qilish organlari tomonidan o’zaro ma’lumot to’plash va almashishni o’z ichiga olishi va ruxsat berishi kerak.

Kiberterrorizmga qarshi kurashish uchun xalqaro huquqiy bazani yaratishdagi har qanday kechikish kiberterrorchilarga hukumatlar va xalqaro agentliklar ularni qonuniy ta’qib qilish imkoniyati cheklangan yoki umuman imkoni yo’qligi haqida aniq xabar beradi. Xalqaro huquqiy baza yaratilganidan keyin ham asosiy muammolar huquqni muhofaza qiluvchi organlar tomonidan politsiya faoliyati va bunday jinoyatlarni fosh etishda bo‘ladi.

FOYDALANILGAN ADABIYOTLAR:

1. Appathurai, J. (2007). North Atlantic Treaty Organization [Press Briefing], Retrieved from accessed on 30 September 2012
2. Attorney-General’s Department. (2010). Critical infrastructure resilience strategy. Canberra: Commonwealth Of Australia.
3. Attorney General for Australia 2012 – New laws in the fight against cyber crime, 22 August 2012. Retrieved accessed on 30 September 2012
4. Australian Crime Commission, (2011). Cyber crime. Retrieved from September 2012
5. Australian Security Intelligence Organization [ASIO]. (n.d.). ASIO Report to Parliament 2010–11. Retrieved from accessed on 30 September 2012
6. Convention on Cybercrime, n.d – Summary. Retrieved from of Europe, n.d. accessed on 30 September 2012
7. Council of Europe, n.d., Retrieved from accessed On 30 September 2012
8. Criminal Code Act 1995 (Cth)

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-5

9. Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002 (Cth)

10. Cybercrime Act 2001 (Cth)

11. Cybercrime Legislation Amendment Bill 2011(Cth)

12. Department of the Prime Minister and Cabinet. (2012). The National Security and International Policy Group Executive. Retrieved from accessed on 30