

KIBERTERRORIZMGA QARSHI KURASHDA XALQARO TAJRIBA

Asamatdinov Ergash

Nukus davlat pedagogika institute falsafa fanlari nomzodi.

<https://doi.org/10.5281/zenodo.15280624>

Annotatsiya. Maqolada kiberterrorizm transchegaraviy xususiyatga ega bo'lganligi sababli, uning ko'rinishlari davlatlar o'rtasidagi munosabatlarning yomonlashishiga, iqtisodiy va diplomatik aloqalarning buzilishiga, davlatlararo tashkilotlar faoliyatiga to'sqinlik qilishi mumkinligi masalalari muhokama qilinadi.

Kiberterroristik harakatini amalga oshirish uchun turli hil usullar foydalanish mumkinligi, asosan, kiberhujum, kiberterror akti, kiberjinoyat, kibernakon kabi tushunchalar tafsiflanadi. Shuningdek, bugungi kunda kiberterrorizm tahdidi turli davlatlarni unga qarshi kurashda hamkorlik qilishga ehtiyojining ortib borishida alohida o'rin tutadi.

Kalit sózlar: kiberterrorizm, kiberhujum, kiberterror akti, kiberjinoyat, kibernakon, aqlli qurilmalar, xatti-harakatlar, kiberkosmik, viruslar, virtual, shifr, kod, dezinformatsiya, shaxs, jamiyat.

МЕЖДУНАРОДНЫЙ ОПЫТ БОРЬБЫ С КИБЕРТЕРРОРИЗМОМ

Аннотация. В статье рассматриваются такие вопросы, как кибертерроризм имеет трансграничный характер, а его проявления могут ухудшать отношения между странами, нарушать экономические и дипломатические отношения, препятствовать деятельности межгосударственных организаций. Для осуществления кибертеррористических действий могут использоваться разные методы, в основном описаны такие понятия, как кибератака, кибертеррористический акт, киберпреступность, киберпространство. Также сегодня угроза кибертерроризма занимает особое место среди растущей потребности различных стран сотрудничать в борьбе с ним.

Ключевые слова: кибертерроризм, кибератака, кибертеррористический акт, киберпреступность, киберпространство, интеллектуальные устройства, грубое поведение, киберкосмос, вирусы, виртуальный, пароль, код, дезинформация, человек, общество.

INTERNATIONAL EXPERIENCE IN COMBATING CYBERTERRORISM

Abstract. The article discusses issues of the fact that cyber terrorism has a cross-border nature, and its manifestations can worsen relations between countries, disrupt economic and

diplomatic relations, and hinder the activities of interstate organizations. Different methods can be used to carry out cyberterrorist actions, mainly concepts such as cyberattack, cyberterrorist act, cybercrime, cyberspace are described. Also, today, the threat of cyber-terrorism occupies a special place in the increasing need of various countries to cooperate in the fight against it.

Key words: *cyberterrorism, cyberattack, cyberterrorist act, cybercrime, cyberspace, smart devices, behavior, cyberspace, viruses, virtual, cipher, code, disinformation, person, society.*

KIRISH

Bugun har bir inson axborot texnologiyalari bilan chambarchas bog'liq, internetdan foydalanuvchilar soni kundan-kunga ortib bormoqda. Yer yuzining deyarli istalgan nuqtasida internetga ulanish imkoni mavjud. Biroq bu "virtual dunyo" turli kuchlar uchun terroristik, ekstremistik tashviqotlar va g'oyalar, o'z qarashlarini ommaga targ'ib qilish, har xil jinoiy to'dalar faoliyatini amalga oshirish yo'lida asosiy qurol sifatida ham qo'l kelmoqda. O'z navbatida global va mintaqaviy xavfsizlikka nisbatan yangi tahdidlar, muammolar yuzaga kelayapti.

Qayd etish o'rinli, kiberterrorizm yangi va o'rganilmagan jinoiy sohadir. Internet tarmog'idagi ochiq manbalar orqali biologik, kimyoviy, hattoki yadro qurollarini tayyorlash texnologiyalarini o'rgangan holda amalga oshirilayotgan terrorchilik harakatlari huquqni muhofaza qiluvchi organlar e'tiborini tortmoqda. Saytlarni noqonuniy yo'llar bilan buzish orqali kiberterrorchilar turli maxfiy ma'lumotlarni olish imkoniga ham ega bo'layotganini aytish joiz.

Tadqiqot metodologiyasi

Kiberterrorizm aslida axborot texnologiyalari ichki faoliyatiga noqonuniy aralashish, kompyuterda mavjud dasturlar yoki ma'lumotlarni maqsadli ravishda yo'q qilish, zarar keltirish, davlat organlarining muhim qismlari faoliyatini izdan chiqarish, shu bilan birga, insonlar hayotiga xavf solish, moddiy zarar keltirish yoki ommaviy qo'rqitish, harbiy nizolar kabi turli zararli oqibatlarini keltirib chiqarishga qaratilgan xatti-harakatdir.

Kiberterrorizm shiddat bilan o'sib borishining yana bir sababi, u qurol-yarog' yordamida amalga oshiriladigan terrorchilik harakatidan arzonga tushadi, jangovar harakatlar, xunrezliklar bo'lmaydi. Buzg'unchi harakatlar internet va ijtimoiy tarmoqlardan foydalangan holda amalga oshiriladi.

Internet tarmog'i o'zining ochiqligi, tezkorligi va tejamkorligi, nazoratning sustligi yoki umuman yo'qligi, dunyo bo'ylab foydalanuvchilari borligi, axborotlarning tez va arzon yo'l bilan to'liqligicha tarqalishi, hamfikir guruhlarni tashkil etish mumkinligi, aloqalarning anonim ekani, asl manbani aniqlash imkoni yo'qligi, strategik ob'ektlar, harbiy tashkilotlar kompyuterlariga noqonuniy ulanish imkoni mavjudligi, tarmoqlarning yashovchanligi bilan terrorchi tashkilotlarni o'ziga jalb qilmoqda.

“Dunyoda terrorizm tahdidlari, ayniqsa, so'nggi yillarda kuchayib borayotgani ularga qarshi, asosan, kuch ishlatish yo'li bilan kurashish usuli o'zini oqlamayotganidan dalolat beradi”.[1]

Bugun terrorizm jangarilar yashirib yurgan yoki bosh qarorgohlari joylashgan muayyan davlat hududi bilan chegaralanib qolayotgani yo'q. Ular allaqachon kiberolamga ko'chib ulgurishgan. Terrorchi tashkilotlar o'z saflarini kengaytirish hamda maqsadlariga erishishda texnika va internetning so'nggi imkoniyatlaridan ustomonlik bilan foydalanayapti. Shu yo'l bilan terrorchilik harakatlari, maqsad va vazifalari haqida ma'lumot berish, o'z g'oya va mafkurasini omma orasida tarqatish bilan birga internet foydalanuvchilariga axborot-psixologik ta'sir o'tkazish, odamlar o'rtasida vahima uyg'otish, terrorchilik harakatlarini qo'llab-quvvatlash uchun mablag' yig'ish, zaharli moddalar, portlovchi vosita va qurilmalar hamda ularni tayyorlash texnologiyasini o'rgatish, terrorchilik tashkiloti safiga yangi a'zolari qabul qilish singari harakatlarni amalga oshirishmoqda.

Ushbu jihat keyingi 5-6 yilda dahshatli oqibatlar keltirgan IShID terrorchilik tashkiloti faoliyatida yaqqol ko'rindi. Ular o'z tizimida g'oya va maqsadlarni targ'ib qilish bilan shug'ullanuvchi mutaxassislarni birlashtirgan alohida tuzilma tashkil etishdi. Bugungi kunda internetda tarqatilayotgan bu kabi ma'lumotlarning 80 foizi Yaqin Sharq hududlarida faoliyat yuritayotgan terrorchi tashkilotlarga tegishlidir.

OAV ma'lumotlari tahlili hamda jabrlanuvchilarning iqrorlariga ko'ra, radikal g'oyalarning tarqatilishi va tashkilotlarga yollash harakatlarining aksariyati "Facebook", "Odnoklassniki", "Vkontakte", "Twitter", "Youtube" kabi ijtimoiy tarmoqlarda amalga oshirilmoqda.

Hozir psixologik jihatdan ishlov berilgan, jangarilarning ekstremistik, aqidaparastlik g'oyalari bilan yo'g'rilgan videoroliklari bilan bir qatorda mobil ilovayu, terrorchilar belgisi aks ettirilgan buyumlarni sotib olish imkonini beruvchi elektron do'konlar ko'payib borayotgani ham kiberterrorizmning tarkibiy unsurlariga aylangan.

Biz ana shunday xavfdan ogoh bo'lishimiz, farzandlarimizni ularning ta'siridan har tomonlama himoya qilishimiz lozim. [2]

Ekspertlarning xulosasiga ko'ra, bu rivojlanayotgan davlatlarning taraqqiyotiga ko'maklashish, umuminsoniy demokratik tamoyillarni qaror toptirish niqobi ostida fuqarolar ongiga ta'sir o'tkazish, ularni turli yo'llar bilan o'z maqsadlari sari bo'ysundirish orqali amalga oshirilmoqda.

Afsuski, bu jarayonda kiberhujumlarni uyushtirish, bu yo'lda internet global tarmog'ining mislsiz imkoniyatlaridan «samarali» foydalanishga urinishlar tobora avj olmoqda.

Xususan, ular kiberjinoyatchilikka qarshi kurash faoliyatida O'zbekiston Respublikasi va uning xalqini axborot texnologiyalari va kommunikatsiyalari orqali amalga oshirilayotgan yoki bunga imkon berayotgan shaxs, jamiyat va davlat xavfsizligini va ularning manfaatlari tashqi hamda ichki kibertahdidlardan himoya qilinishini ta'minlash, mazkur sohada qonuniylik va qonun ustuvorligini mustahkamlash, kiberjinoyatlar va kiberhuquq buzarliklarning oldini olish, ularni aniqlash va barham berish kabi vazifalarni amalga oshirishi darkor.

Tahlil va natijalar

Shuningdek, kiberjinoyatlar va kiberhuquq buzarliklarni tergov qilish va ularni aniqlash, bartaraf etish hamda oldini olish bo'yicha zarur qarorlar qabul qilish, kiberjinoyatchilikka qarshi kurashish bo'yicha normativ-huquqiy hujjatlar loyihalarini ishlab chiqishda ishtirok etish, kiberterrorizm, kiberekstremizm, uyushgan jinoyatchilikka qarshi kurashish, davlat organlari manfaatlariga hamda kiberxavfsizligiga tahdid soluvchi kiberhatarlarni aniqlash va ularga qarshi kurashish, kiberjinoyatlar bo'yicha tergovga qadar tekshiruv va dastlabki tergovni o'tkazish, tezkor-qidiruv faoliyatini amalga oshirish, fuqarolarning huquq va erkinliklariga tahdid soluvchi kiberjinoyatlarning sodir etilishiga imkon yaratuvchi sabablar hamda shart-sharoitlarni aniqlash va bartaraf etish kabi muhim vazifalarni bajarishlari lozim.[3]

AQSh hukumatining xavfsizlik bo'yicha eksperti Richard Klark o'zining Cyber Warfare kitobida (2010 yil may oyida nashr etilgan) yozganidek, "kiber urush - bu bir davlatning boshqa davlatning kompyuterlari yoki tarmoqlariga zarar etkazish yoki zarar etkazish maqsadlariga erishish uchun kirishi halokat". Britaniyaning The Economist jurnali kibermakonni "quruqlik, dengiz, havo va kosmosdan keyingi urushning beshinchi sohasi" [4] deb ta'riflaydi.

Kiberterrorizmga qarshi kurash siyosatining samaradorligi nafaqat ijtimoiy-siyosiy tizimning barqarorligi virtual makondagi jarayonlar ustidan davlat nazoratining rivojlanishi

ichki va tashqi ushbu segmentdagi huquqiy meyorlarga bog'liqdir. Ko'p jihatdan hukmron elita va mahsus xizmatlarning vakillari tahlil qilingan hodisani tushunish uchun vositalarga ega ekanligi bilan bog'liq bo'lib uni konseptual asoslarini tushunmasdan uslubiy jihatdan to'liq o'rganish imkonini beradigan yondashuvlarni kengaytirib bo'lmaydi.

Kiberterrorizm- bu global tarmoqlarning nazoratsiz ishlatilishi davlat fuqarolik jamiyati va maxsus xizmatlarning siyosatning ushbu segmentiga etarlicha etibor bermasligi kompyuter dasturlari va tarmoqlariga yoki ulrdagi ma'lumotlarga hujumlarda namoyon bo'layotganligi sababli ko'p qirrali hodisadir. Terrorizm faliyati subyektlarining maqsadlari va manfaatlariga erishish yo'lida jamiyatda qo'rquv va umidsizlik muhitini yaratish uchun, unga qarshi samarali kurashish uchun jahon hamjamiyatining say-harakatlarini birlashtirishni talab qiladi.

Xulosa va takliflar

Xulosa shuki, kiberterrorizmga qarshi kurashish bo'yicha samarali siyosatni ishlab chiqish quyidagi asosiy yo'nalishlar bo'yicha amalga oshiriladi: ustuvor maqsadlarni (global mintaqaviy, milliy) va voositalarni aniqlash, yuzaga kelishi mumkin bo'lgan kiberterrorizm tahdidlarini aniqlash, aholini himoya qilish birinchi xalqaro infratuzimani yaratish va muvofiqlashtirish maxsus antiterror dasturlarini xalqaro huquqni va boshqalarni ishlab chiqishni o'z ichiga olgan kiberhujumlarga qarshi kurashish.

REFERENCES

1. O'zbekiston Respublikasi Prezidenti Sh.Mirziyoevning BMT Bosh Assambleyasi 72-sessiyasidagi nutqi. 19 sentyabr 2017 yil
2. No'rmatov B. Kiberjinoyatchilik. Qashqadaryo gv.uz. ma'lumoti asosida. Ijtimoiy. 17.03.2019
3. Iminov A. Kiberjinoyatchilikka qarshi kiberxavfsizlik. 07.04.2022
4. Clarke, Richard A. Cyber War, HarperCollins (2010)