RIVOJLANGAN MAMLAKATLARDA KIBERTERRORIZM: SIYOSIY VA MAFKURAVIY TAHDID

Narzulloyev Mironshoh Elmurodovich
Toshketnt davlat yuridik universiteti
“Xususiy huquq” fakulteti 2-bosqich talabasi
Email: narzullayev200404@icloud.com
Phone: +998-93-681-08-83

Annotatsiya: Kiberterrorchilik bu tahdid yoki qo‘rqitish orqali, internetdan foydalangan holda, siyosiy yoki mafkuraviy muvaffaqiyatga erishish maqsadida uyushtiriluvchi kiber hujumlardir. Kompyuter viruslari , fishing, zararli dasturlar, apparat usullari va dasturlash matnlari kabi vositalar yordamida kompyuter tarmoqlarini, xususan, internetga ulangan shaxsiy kompyuterlarni qasddan va keng miqyosda buzish harakatlari internet terrorizmining ko‘rinishi bo‘lishi mumkin. Yildan- yilga texnologik rivojlanish o’sib borgani sayin kiberterrorizmning butun dunyo bo’ylab yoyilishi yanada jadallashadi.Aynan kiberterrorizm millionlab insonlarning hayoti balki,milliy xavfsizlikni ham xavf osiga qo’yadi.Siyosatchi,jurnalistlar va bir qancha sohalardagi mutaxassislar kiberterrorizm borasida anchagina bahs va munozara yuritishgan.Kiberterrorizm internet aloqalari yordamida qo’rqitish orqali siyosiy yokida mafkuraviy yutuqlarga erishishdir.

Tayanch tushunchalar: Kiberhujum, Kiberdelikt**,** Kiberxavfsizlik siyosati**,** Shaxsiy ma’lumotlarni himoya qilish**,** Axborot xavfsizligi qonunchiligi**,** Kiberhujumlar (hackerlik faoliyati)**,** Raqamli huquqlar**,** Kiberterrorizm**,** Ma’lumotlarga noqonuniy kirish**,** Kiberjinoyatlarni tergov qilish**,** Elektron dalillar.

Ushbu sohadagi dastlabki jinoyatlarga to’xtalmoqchi bo’lsak, 1990-yillarga yuzlanishimiz kerak bo’ladi. Chunki ushbu o’n yilliklarda axborot texnologiyalarining revolyutsiyasi kuzatilgan. Kiberterrorizm atamasi birinchi marta 1980-yillarning o'rtalarida Kaliforniyadagi “Xavfsizlik va razvedka” institutining katta ilmiy xodimi Barri Kollin tomonidan kiritilgan.[1] Aslida kiberterrorchilik xavfi qanchalik real? G’arb davlatlarida muhim infratuzilmalarning aksar qismi kompyuter tarmoqlari orqali tarmoqqa ulanganligi bois, sodir bo‘lishi mumkin bo‘lgan tahdidning ehtimoli har doimgidanda yuqori. Kundalik hayotimizda axborot texnologiyalariga ko’proq suyanar ekanmiz, uning oqibatida yuzaga keladigan turli xil hujumlardan himoyalanish uchun ham o’zimizni tayyorlab borishimiz kerak. Xuddiki uyali

[1] https://www.sciencedirect.com/science/article/abs/pii/S0167404820304181.

aloqalarimizning yangi turlarini almashtirganimiz kabi zamon bilan hamnafas bo’lgan holda yangidan- yangi kiberhujumlardan ogoh bo’lishimiz kerak.

Kiberterrorizmning real xavfi. Kiberterrorizm natijasida hozirgi kunga qadar yetkazilgan zarar juda ham katta miqdorni tashkil etadi. Shu yetkazilgan zararlarni birgina Amerika Qo’shma Shtatlari misolida statistika orqali ko’rsatib ketsak:

-Wannacry cyber attack (2017) qiymati 8 milliard dollar

-Notpetya cyber attack (2017) qiymati 10 milliard dollar

-East coast blizzard (1993) qiymati 10 milliard dollar

-Hurricane Irene (2011) qiymati 12 milliard dollar

-California Wildfires (2018) qiymati 25 milliard dollar

Yuqorida statistikaga nazar tashlasak, shuni guvohi bo’lamizki, dunyoning internet xavfsizligi bo’yicha eng yuqori o’rinlarda turuvchi AQSH davlatida ham kiberhujumlar natijasida davlatga juda katta zarar keltirilgan. Jahon miqyosida bir qancha kiberhujumlardan namunalarga yuzlanamiz, masalan, AQSHda Pentagonning va Gavayidagi Tinch okeani qo’mondonligining internet xavfsizligi sifatini tekshirish maqsadida AQSH hukumatining o’zi rozilik berib ikkita xakerlar jamoasini yollashgan. Ushbu loyihaga NSA (National Security Agency) Milliy Xavfsizlik Xizmati rahbarlik qilgan. Xakerlar guruhlariga Pentagonning istalgan tarmog’idan foydalanishga ruxsat berilgan. Faqatgina AQSH hukumati tomonidan qabul qilingan qonunlarga zid keladigan xatti-harakatlarni amalga oshirmasliklari so’ralgan, xolos. Jamoalar o’zlarini rasmiylarcha yoki texnik xodim sifatida tutib bildirmasdan Maxfiylik Xizmati xodimlaridan osongina parollarni qo‘ kiritib, o’nlab tizimlardagi profillarini buzib kirib, o’chirishgan yoki yangilarini yaratishgan. Kiberterrorizm predmetini keltirib chiqaradigan barcha xavotirli statistik ma’lumotlar orasida bitta oddiy statistikani eslatib o’tish kerakki,hozirgacha AQSH jamoat obyektlari, transport tuzilmalari,yadroviy stansiyalar,elektr tarmoqlari yoki milliy infratuzilmaning boshqa asosiy komponentlarida hech qanday jinoyat terroristlar tomonidan sodir etilmagan. Kiberterrorizmda boshqa davlatning siyosiy va iqtisodiy manfaatlarini ko’zlovchi ma’lumotlarni o’g’irlash,saqlash va shu orqali tahdid qilishni rejalashtirish ham kiberterrorizmning tarkibiy elementi hisoblanadi.Masalan,AQSH armiyasi Al-Qoida terroristik guruhining kompyuterlarini tarmoqlarini tekshirishganida AQSH yadro qurollari omborlari, Yevropa magistral suv quvurlarining maxfiy koordinatalarini topishgan.

2014-yil noyabr oyida Sony Pictures Entertainment (SPE) ga qilingan hujum nafaqat korporativ ma’lumotlarning o‘g‘irlanishi, balki kino sanoatining va davlat-diplomatiyaning kesishish nuqtasida qiziqarli va xavfli misol bo‘ldi. “Guardians of Peace” nomli guruh SPE tarmoqlariga kirib, yuzlab xodimlar, ijodkorlar va hamkorlarga tegishli elektron pochta, shaxsiy ma’lumotlar va hali chiqarilmagan filmlar — jumladan The Interview filmi nusxalarini ommaga e’lon qildi. Shu bilan

birga, tizimlarni falaj qiluvchi “wiper” turidagi zararli dasturlar qo‘llanilib, kompaniya ichki infratuzilmasiga sezilarli zarar yetkazildi. [2]Voqea siyosiy rang-rohga ega bo‘lishi bilan ham e’tibor qozondi: hujumchilar The Interview filmining namoyish etilishiga qarshi tahdidlar bildirdi, natijada aksariyat kinoteatr zanjirlari premyerani bekor qildi yoki chekladi — bu esa so‘z erkinligi, madaniy mahsulotni tarqatish va korporativ qarorlar o‘rtasidagi murakkab bog‘liqlikni ko‘rsatdi. AQSh hukumati bu hujumni milliy xavfsizlik nuqtai nazaridan jiddiy baholab, FBI va boshqalar texnik tahlil asosida bu faoliyatni Shimoliy Koreya bilan bog‘lagan. Shu sababli administratsiya ma’lum choralar, jumladan iqtisodiy sanksiyalarni joriy etdi.

2016-yilga yaqinlashganda, rivojlangan davlatlarning saylov jarayonlarida tahdidning yangi shakli kuzatila boshlandi — raqamli hujumlar va axborot kampaniyalari orqali siyosiy barqarorlikka aralashuv. APT28 (Fancy Bear) va APT29 (Cozy Bear) nomlari bilan tanilgan Rossiyaga aloqador xaker guruhlari, ayniqsa, AQSh va Yevropadagi demokratik saylov jarayonlariga bevosita ta’sir ko‘rsatgani aniqlangan. Misol uchun, 2016-yilda AQShdagi saylovlar chog‘ida APT29 guruhining 2015-yil iyul oyida Democratic National Committee (DNC) tarmog‘iga spear-phishing usuli orqali kirgani ma’lum: bu usulda xakerlar e-pochta orqali tayyorlangan hiyla bilan xodimni aldab, parolini qo‘lga kiritgan. Keyin esa APT28 esa 2016-yil mart oyida John Podestaning e-pochtasiga kirish imkoniga ega bo‘lib, saylov kampaniyasi tarmog‘i ichida ma’lumot o‘g‘irlagan.[3]

AQShning Adliya vazirligi 2018-yil iyul oyida Rossiyaning harbiy razvedka organi (GRU)ga bog‘liq 12 nafar rus fuqarosiga “2016-yilgi saylovga kiberhujum” ayblovlari qo‘yilganini e’lon qilgan. Bu hujjatda ular DNC, Democratic Congressional Campaign Committee (DCCC) va boshqa siyosiy agentliklarning tarmoqlariga kirgan, soxta domenlar va bitcoin orqali moliyalashtirilgan operatsiyalarni amalga oshirganligi bildirildi.

Shuningdek, hujum ishlab chiqilgan soliqlashuv bilan emas, balki uzoq muddatli reja asosida bo‘lgan: bank, moliya, strategik infratuzilma yoki saylov texnologiyalari emas, balki kampaniyalar, partiyalar, agentliklar va ommaviy axborot vositalariga yo‘naltirilgan. Ma’lumotlar shuni ko‘rsatadiki: xakerlik orqali saylov natijalarini bevosita o‘zgartirishdan ko‘ra — saylovchilarning onglariga ta’sir qilish, ularning ishonchini susaytirish, demokratik jarayonga shubha qo‘yish maqsad qilingan

Kiberterrorizmning shakllari:

Maxfiylik qonuni - bu shaxsning va shaxsiy makoniga daxlsizlik qilish huquqini tan olishdir. Shaxsiy daxlsizlik huquqi mustaqil va o'ziga xos tushuncha sifatida

[2] https://frameworksecurity.com/post/the-sony-pictures-breach-a-deep-dive-into-a-landmark-cyber-attack.

[3] https://securingdemocracy.gmfus.org/incident/russian-government-backed-hackers-target-american-political-parties-organizations-and-campaigns-in-the-2016-presidential-election/.

huquqbuzarlik to'g'risidagi qonun sohasida paydo bo'lgan, unga ko'ra shaxsiy hayotga noqonuniy tajovuz natijasida yetkazilgan zararni qoplash uchun yangi da'vo sababi e'tirof etilgan. Biroq so'nggi paytlarda bu huquq konstitutsiyaviy maqomga ega bo'lib, uning buzilishi tegishli qonunlarga muvofiq ham fuqarolik, ham jinoiy oqibatlarga olib kelmoqda.. Axborot texnologiyalarining paydo bo'lishi bilan shaxsiy daxlsizlik huquqining an'anaviy tushunchasi boshqa huquqiy nuqtai nazarni talab qiladigan yangi o'lchovlarni oldi. Ushbu muammoni hal qilish uchun “Axborot texnologiyalari to'g'risida”gi qonunning 2000-yildagi resurslaridan foydalanish mumkin. Qonunning turli qoidalari fuqarolarning internet tarmoqlaridagi shaxsiy huquqlarini to‘liq himoya qiladi. Fuqarolarning shaxsiy daxlsizligi huquqlariga tajovuz qilish tendensiyasiga ega bo'lgan ayrim xatti-harakatlar huquqbuzarliklar va qonunbuzarliklar sifatida tasniflanadi.

Axborot texnologiyalari qimmatli davlat sirlari va xususiy tashkilotlar, hukumat va uning idoralari ma'lumotlarini o'zlashtirish uchun suiste'mol qilinishi mumkin. Hukumatga tegishli bo'lgan kompyuter tarmog'ida mudofaa va boshqa o'ta qattiq muhofaza etiladigan sirlarga taalluqli qimmatli ma'lumotlar bo'lishi mumkin, buni esa hukumat boshqacha tarzda baham ko'rishni istamaydi. Xuddi shu narsa xakerlar tomonidan o'z faoliyatini osonlashtirish, jumladan, mulkni yo'q qilish uchun nishonga olinishi mumkin.

Elektron boshqaruvning maqsadi fuqarolarning davlat idoralari bilan o'zaro aloqalarini muammosiz hal qilish va axborotni erkin va oshkora almashishdir. Demokratik davlatda odamlar agar ijtimoiy,siyosiy,iqtisodiy va boshqa muammolardan xabardor bo’lmasalar, o’zlariga nisbatan qo’llanilishi mumkin bilgan real kiberhujumlardan himoyalana olmaydilar. Axborot olish va tarqatish huquqi so'z erkinligi bilan bog'liq tushunchalar hisoblanadi. Biroq, axborot olish huquqi mutlaq emas, bu hukumat tomonidan jamoat manfaatlarini ko'zlab o'rnatishi mumkin bo'lgan oqilona cheklovlarga bog'liq.

Kiberterrorchilar, shuningdek, hukumat va uning agentliklarining elektron bazalarini yuklash uchun tarqatilgan xizmatlardan voz kechish (DDOS) usulidan foydalanishlari mumkin. Bu birinchi navbatda bir nechta himoyalanmagan kompyuterlarni virus hujumlari yo'li bilan buzish va keyin ularni nazorat qilish orqali mumkin bo'ladi. Nazorat qo'lga kiritilgandan so'ng, ular terrorchilar tomonidan istalgan hududdan manipulyatsiya qilinishi mumkin. Ushbu zararlangan kompyuterlar ma'lumot yoki talabni shunchalik ko'p miqdorda yuborish uchun yaratilganki, qurbonning serveri ishdan chiqadi. Bu hukumat va uning idoralariga katta moddiy va strategik yo'qotishlarga olib keladi. Shuni ta'kidlash kerakki, minglab buzilgan kompyuterlar bir vaqtning o'zida bitta hostga hujum qilish uchun ishlatilishi mumkin, bu esa uning elektron mavjudligini haqiqiy va qonuniy fuqarolar va oxirgi foydalanuvchilar uchun ko'rinmas qiladi.

Kiberterrorchilik faoliyatining asosiy maqsadi tarmoqlarga zarar yetkazish va ularning uzilishidir. Bu faoliyat xavfsizlik idoralarining e'tiborini hozircha chalg'itishi mumkin, bu esa terrorchilarga qo'shimcha vaqt beradi va ularning vazifalarini nisbatan osonlashtiradi. Bu jarayon kompyuterni buzish, virus hujumlari, xakerlik va hokazolarning kombinatsiyasini o'z ichiga olishi mumkin. Kiberterrorizm borasida bir qancha izlanishlar o’tkazilgan. Shularning eng asosiylaridan biri bu Jim Lewisning “Kiberterrorizm, kiber urush va boshqa kibertahdidlar xavfini baholash”[4]. Bu izlanishda, “Xakerlar xalqni tiz cho'ktirmoqchi, degan g'oya juda uzoqqa cho'zilgan jiddiy qabul qilinishi kerak bo'lgan ssenariy", dedi Lyuis. “Xalqlar avvalgilariga qaraganda kuchliroq kiberterrorizm va kiber urush bo'yicha qarashlarga ega. Ular xizmatni tiklashda dastlabki tahlilchilarga qaraganda ancha moslashuvchan va sezgir. Ko'pgina kompyuter xavfsizligi bo'yicha mutaxassislar internetdan foydalanish natijasida millionlarning o’limiga olib kelishiga jahon amin bo‘lmoqda. Shunday qilib, masalan, Mudofaa vazirligi zaif tizimlarni himoya qiladi, ularni internetdan va hatto Pentagonning ichki tarmog'idan ajratib qo'yish orqali. Markaziy razvedka boshqarmasining tasniflangan kompyuterlari, Federal qidiruv byurosining butun kompyuter tizimi kabi havo bo'shlig'iga ega. Kiberterrorizm bugun va ertaga: Hozirgi kunda kiberterrorizm tahdidi bo'rttirilgan deyish oddiyroq ko'rinadi. Kiberterrorizmning yagona holati hali qayd etilmagan; AQSh mudofaasi va razvedkasi kompyuter tizimlari havo bo'shlig'i shuning uchun ham internetdan ajratilgan;vinternet aloqalari orqali boshqariladigan tizimlar xususiy kompaniyalar hujumga ko'proq moyil bo'ladi, lekin ular taxmin qilinganidan ko'ra ko'proq chidamli; kiberhujumlarning ko'pchiligi xakerlar tomonidan, agar mavjud bo'lsa, siyosiy jihatdan kam maqsadlar va terroristlar maqsad qilgan tartibsizlik va qirg'in keltirish istagi yo'q. Shunday ekan, nima uchun nisbatan kichik tahdid haqida shunchalik tashvish bildirildi? Sabablarini endi keltirib o’tamiz. Birinchidan, Danning ta'kidlaganidek, "kiberterrorizm va kiberhujumlar hozir o’zining cho’qqisida. Ikkinchidan, ommaviy axborot vositalari ko'pincha kiberhujum va kiberterrorizm o'rtasidagi farqni ajrata olmaydi. Kiberterrorizm va uning tahdidini noto'g'ri o'xshashliklardan kelib chiqib bo'rttirib ko'rsatadi.masalan: "Agar o'n olti yoshli bola kiberhujum qila olsa, yaxshigina moliyalashtirilgan terroristik guruh nimalarga qodir deb o’ylaysiz? Uchinchi omil, Grinning ta'kidlashicha, kiberterrorizm ikki sohada ifodalanadi - terrorizm va texnologiya. Buni juda ko'p odamlar, shu jumladan ko'pchilik qonunchilik tashabbusi bilan chiqayotganlar va yuqori martabali ma'muriyat xodimlari to'liq tushunmaydilar va shuning uchun qo'rqishadi.Beshinchi omil - bu tushunmovchilik, "kiberterrorizm" atamasi sun’iy ravishda jamoatchilikni sarosimaga solgan va son- sanoqsiz afsonalarni paydo bo'lishiga sabab bo'lgan. Undan

[4] https://oversight.house.gov/wp-content/uploads/2012/01/5-25-11_Lewis_NatSec_Testimony.pdf.

tashqari kiberterrorizm bir qancha muammolarni keltirib chiqarmoqda. Masalan, kiberterrorizm internetning chegara bilmas tarmoq bo’lganligi tufayli katta yurisdiksiyaviy muammolarni keltirib chiqaradi. Hujum bir joydan kelib, boshqasiga ta'sir qilganda qaysi qonunlar va hokimiyatlar qo'llanilishini aniqlash murakkab bo'lishi mumkin. Bu mas'uliyatni yuklash, huquqbuzarlarni javobgarlikka tortish va xalqaro choralarni muvofiqlashtirishda qiyinchiliklar tug'diradi. Turli huquqiy tizimlar, kiber qonunlarning turlicha talqini va ekstraditsiya shartnomasidagi cheklovlar jarayonni yanada murakkablashtiradi. Ushbu yurisdiksiyaviy muammolarni hal qilish mening naznimda xalqaro hamkorlikni kengaytirish, yangilangan qonunchilik bazasi va chegaralar osha kiberterrorizmga qarshi samarali kurashish uchun ko‘p tomonlama kelishuvlarni talab qiladi.

Xulosa. Kiberterrorizm zamonaviy dunyoda muhim va ancha shakllangan muammolarni keltirib chiqaradi. Kibermakondagi jinoyatchilar esa texnologik imkoniyatlardan imkon boricha foydalanib muhim infratuzilmalarga,iqtisodiyot va hatto shaxsiy daxlsizlikka qaratilgan jinoyatlarni amalga oshirishmoqda.Men keyingi yillardagi shiddatli rivojlanish va keyingi 5 yil o’tgan 30 yillik texnologik o’sishdan keskinlashishini hisobga olgan holda kibermakondagi ko’p qirrali global muammolarni hal qilish xalqaro hamkorlikni,innovatsion texnologik yechimlarni,mustahkam kiberxavfsizlik choralarini hamda tahdidlardan himoyalanish va raqamli erkinliklarni qo’llab- quvvatlash o’rtasidagi muvozanatni talab qilishi kerakligini hamda dunyo bo’ylab kiberhujum qurbonlarini kamaytirish va oldini olish uchun kibersavodxonlikni yangi darajaga ko’tarilishi kerakligini,buning uchun universtitetlarda alohida yo’nalishlar tashkil qilinishi kerak deb o’ylayman. Kiberhujumlar ko’paya borar ekan,u keltirib chiqaradigan xavflarni yumshatishda faol choralar va moslashuvchanlik muhim ahamiyatga ega bo’ladi. Mazkur muammoga yechimni huquqiy tomondan izlasak,avvalambor joriy qonunchilikni yangilab borish kerak. Huquqbuzarlik normalarini belgilash, jazo tayinlash hamda ta’qib masalalari ushbu yangi sohada o’z qonuniy tasdig’ini topishi kerak. Ikkinchidan, kiberterrorizm bilan bog’liq hollarda mamlakatlar o’rtasida samarali ma’lumot almashish imkonini beradigan shartnomalar tuzilishi kerak. Uchinchidan, eng muhimi, kibermakonda yurisdiksiyani aniqlash uchun aniq yo’riqnomalarni ishlab chiqish, hujum qayerdan kelib chiqishi yoki ta’siridan qat’i nazar, samarali qonuniy choralar ko’rishni ta’minlash kerak. To’rtinchidan, davlatxususiy sherikligi: Hukumatlar, huquqni muhofaza qilish idoralari va xususiy sektor subyektlari o'rtasida tahdidlar bo'yicha razvedka ma'lumotlarini almashish va kiber tahdidlarga qarshi jamoaviy mudofaani kuchaytirish uchun hamkorlikni rivojlantirish. Beshinchidan, global kiberxavfsizlik standartlari: davlatlar bo'ylab xavfsizlik choralarining asosini ta'minlash uchun global kiberxavfsizlik standartlarini ishlab chiqish va qabul qilishni rag'batlantirish. Oltinchidan, raqamli sud ekspertizasi: kiberterrorizm holatlari bo'yicha dalillarni samarali to'plash uchun raqamli sud-tibbiyot

ekspertizasi imkoniyatlarini yaratish, dalillarni aniqlash va ta'qib qilishda yordam berish. Yettinchidan,fuqarolik erkinliklari kafolatlari: xavfsizlik choralarini fuqarolik erkinliklarini himoya qilish bilan muvozanatlash, buning oldini olish va kiber terrorchilarda gumon qilinganlarga qarshi qonuniy harakatlarni ta'minlash.Agarda yuqorida ko’rsatilgan takliflar va o’zgartirishlar qonunchilikka kiritilsa hamda xalqaro miqyosda mamlakatlar erkin ma’lumot almashinuvini yo’lga qo’ysa, kiberhujumlar ortiq muammo bo’lmay qoladi.

References:

1. **Jon Bateman**-Carnegie Europe Xalqaro Tinchlik jamg’armasining texnologiya va xalqaro aloqalar dasturining kata ilmiy xodimi// “Kiber sug’urtada urush,terrorizm va falokat:istisnolarni tushunish va isloh qilish” **[War,terrorism,and catastrophe in Cyber Insurance:Understanding and reforming exclusions]** maqolasi//Nashriyot:**Carnegie Europe,USA**,2020-yil,5-oktabr.Pp.1-5 (in English)
2. **Gabriel Weimann**-Haifa universiteti xalqaro aloqalar professori,Vudro Vilson olimlar markazi sobiq xodimi// “Kiberterrorizm:Tahdid qanchalik real?” **[Cyber terrorism:How is real the threat?]** maqolasi//Nashriyot:**United States institute of peace,USA**,2004-yil dekabr.Pp.1-11 (in English)
3. **Shandler R,Gross ML,Backhaus S**-School of political science,University of Haifa,Department of Psychology,University of Konstanz-“Kiberterrorizm va qasos uchun jamoatchilikning qo’llab-quvvatlashi”**[Cyber terrorism and public support for retaliation.A multi-country survey experiment]**maqolasi//Nashriyot:**British journal of political science,UK**,2022- yil.Pp.852-859 (in Enlish)