

RAQAMLI SOYA. KIBERSTALKING MUAMMOSI

Hamroyev Izzatillo

Toshkent davlat yuridik universiteti.

izzatillohamroyev10@gmail.com

ORCID;0009-0003-4131-4655.

<https://doi.org/10.5281/zenodo.14165537>

Annotatsiya. Kiberstalking – bu zamonaviy raqamli muhitda insonlar uchun jiddiy tahdid solayotgan hodisalardan biridir. Ushbu maqolada kiberstalkingning kelib chiqishi, tarqalishi va uning ijtimoiy va psixologik oqibatlarini tahlil qilinadi. Maqolaning asosiy maqsadi – kiberstalking tahdidlarini aniqlash va unga qarshi kurash strategiyalarini ishlab chiqishga ko‘maklashishdir.

Maqola kiberstalking fenomenini chuqurroq tushunishga, kiberstalking faoliyatlarini monitoring qilish, himoya qilish texnologiyalari va qonunchilikdagi imkoniyatlarni ko‘rib chiqishga qaratilgan. Natijalarda kiberstalkingning shaxsiy xavfsizlikka salbiy ta’siri va jamiyatdagi stress darajasini oshirish omillari aniqlanadi. Tadqiqot natijalari kiberstalkingning oldini olish bo‘yicha amaliy tavsiyalar beradi va shu bilan birga, raqamli tahdid muammosini hal qilishda texnologik himoya usullari, qonuniy asoslar va ijtimoiy ongni oshirishning ahamiyati tahlil qilinadi.

Kalit so‘zlar: kiberstalking, kiberxavfsizlik, shaxsiy ma’lumotlarni himoya qilish, raqamli xavf-xatarlar, virtual makon, IP manzil.

DIGITAL SHADOW. THE PROBLEM OF CYBERSTALKING

Abstract. Cyberstalking is one of the phenomena that seriously threatens people in the modern digital environment. This article analyzes the origins, prevalence, and social and psychological consequences of cyberstalking. The main purpose of the article is to identify threats of cyberstalking and to help develop strategies to combat it. The article is aimed at a deeper understanding of the phenomenon of cyberstalking, monitoring of cyberstalking activities, protection technologies and opportunities in legislation. The results reveal the negative impact of cyberstalking on personal security and factors that increase the level of stress in society. The results of the study provide practical recommendations for the prevention of cyberstalking and, at the same time, analyze the importance of technological protection methods, legal frameworks and social awareness in solving the problem of digital threats.

Key words: cyberstalking, cyber security, personal data protection, digital risks, virtual space, IP address.

ЦИФРОВАЯ ТЕНЬ. ПРОБЛЕМА КИБЕРСТАЛКИНГА

Аннотация. Киберсталкинг – одно из явлений, представляющих серьезную угрозу для людей в современной цифровой среде. В данной статье анализируются истоки, распространенность, а также социальные и психологические последствия киберпреследования. Основная цель статьи — выявить угрозы киберпреследования и помочь разработать стратегии борьбы с ними. Статья направлена на более глубокое понимание феномена киберпреследования, мониторинга киберпреследующей деятельности, технологий защиты и возможностей в законодательстве. Результаты раскрывают негативное влияние киберпреследования на личную безопасность и факторы, повышающие уровень стресса в обществе. Результаты исследования дают практические рекомендации по предотвращению киберпреследований и в то же время анализируют важность технологических методов защиты, правовой базы и общественной осведомленности в решении проблемы цифровых угроз.

Ключевые слова: киберсталкинг, кибербезопасность, защита персональных данных, цифровые риски, виртуальное пространство, IP-адрес.

I. Kirish

Bugungi kunda hayotimizning barcha jabhalariga chuqur kirib kelgan texnologiyalar inson xavfsizligi va maxfiyligi tushunchalarini yangi tahdidlar ostiga qo'yimoqda. Ana shunday tahdidlar orasida kiberstalking (virtual makonda ta'qib) alohida xavfli ko'rinish sifatida ajralib turadi.

An'anaviy stalking odatda jismoniy chegaralar bilan cheklanib qolsa, kiberstalking internet imkoniyatlaridan foydalanib, tajovuzkorlarga masofadan, ko'pincha anonim va izchil tarzda qurbonlarining shaxsiy hayotiga tajovuz qilish imkonini beradi. Virtual makondagi kibertahdidlarning mavjudligi bugungi kunda asosiy ijtimoiy muammolardan biriga aylanib, falsafiy jihatdan mazkur muammoni tahlil etish dolzarb ahamiyat kasb etib bormoqda.

Kiberstalking - kiberzo'ravonlikning bir turi bo'lib, alohida shaxsni, shaxslar guruhini yoki tashkilotni bezovta qilish, ta'qib qilish maqsadida Internet yoki boshqa raqamli vositalardan foydalanish hisoblanadi.¹ Kiberstalking umumiy stalking (inglizcha – bu biror shaxs yoki guruh tomonidan boshqa shaxsga nisbatan istalmagan yoki istalgan tarzda takroriy kuzatish, ta'qib) huquqbuzarligining shakli bo'lib, kibermakonda sodir etilishi bilan xarakterlanadi. Bunday ta'qib qilishda, jinoyatchilar elektron pochta, ijtimoiy tarmoqlar, xabar yuborish, bloglar yoki forumlar kabi vositalardan foydalangan holda qurbonni izlab, doimiy ravishda harakat qiladilar.

¹ Cyberstalking". Oxford University Press. – Oksford universiteti lug'ati ta'rifi

Ular qurbonning internetdagi harakatlarini kuzatib boradi, unga tahdidlar yuboradi, va hatto qurbonni yolg'iz va zaif his qilishiga sabab bo'lgan ta'sirlar yaratadi. Kiberstalkingning yana bir o'ziga xos xususiyati shundaki, bu jarayon jismoniy chegaralarni bilmaydi va texnologiyaning kuchidan foydalanib, har qanday vaqtda, istalgan joyda amalga oshirilishi mumkin. Tajovuzkorlar kibermakonda turgan holda qurbonni ko'rmasdan va uning shaxsiy hayotiga bevosita aralashmasdan, psixologik bosim o'tkazishadi. Bu esa qurbonning ruhiy holatini izchil ravishda buzib, stress, uyat, xavotir, qo'rquv va hatto depressiya kabi salbiy holatlarga olib keladi. Aksariyat hollarda kiberstalkerlar (kiberstalking amalga oshiruvchi shaxslar) o'z qurboniga notanish bo'ladi.

Ya'ni anonimlik kiberstalkingning o'ziga xos xususiyati hisoblanadi. Kiberstalking tushunchasi ko'p hollarda kibertahdidning boshqa turlari sanaladigan kiberbulling, kibexarrasment, doksing kabilar bilan o'xshash tarzda tariflanadi. Shundan kelib chiqib aytishimiz mumkinki, kiberstalking, kiberbulling jismoniy stalkingning aralashmasi sifatida namoyon bo'ladi. Ushbu onlayn taqib shaxsning ma'lumotlaridan foydalangan holda unga elektron pochta, ijtimoiy tarmoqdagi xabarlar orqali hujum qiladi va odatda bu muntazam yoki takroriy, oldindan rejalashtirilgan va qat'iy xarakterda bo'ladi.²

II. Metodologiya

Ushbu tadqiqotda kiberstalkingning jamiyatga ta'sirini tahlil qilish uchun kesma tadqiqot (cross-sectional study) qo'llanildi. Bu tadqiqotda, kiberstalking hodisasini keng ko'lamda tahlil qilish maqsadida, so'rovnoma va ma'lumotlar tahlili usullari qo'llanildi.

Tadqiqot Populyatsiyasi va Ishtirokchilar

Tadqiqot populyatsiyasini kiberstalking hodisasiga duch kelgan va internetdan faol foydalanuvchi shaxslar tashkil etdi. Tanlov tasodifiy ravishda amalga oshirildi, va jami 500 nafar ishtirokchi jalb qilindi. Ishtirokchilarning yoshi, jinsi va ijtimoiy holatiga ko'ra kiberstalkingga nisbatan munosabatlaridagi farqlar tahlil qilindi.

Ma'lumotlarni To'plash

Tadqiqot ma'lumotlari so'rovnoma yordamida to'plandi. So'rovnoma ikki qismdan iborat bo'lib, birinchi qismda ishtirokchilarning demografik ma'lumotlari (yoshi, jinsi, ta'lim darajasi) o'rganildi. Ikkinchi qismda esa kiberstalking bilan bog'liq tajribalar, uning ta'siri va kibexavfsizlik choralari haqidagi savollar berildi.

Ma'lumotlarni Tahlil Qilish

To'plangan ma'lumotlar statistik tahlil dasturlari orqali qayta ishlanib, kiberstalkingning jamiyatdagi o'rni va u bilan bog'liq xavflar tahlil qilindi.

² <https://www.verywellmind.com/what-is-cyberstalking-5181466>

Deskriptiv statistika usuli orqali respondentlarning umumiy holati, jinsiy va yosh bo'yicha farqlari aniqlandi. Chi-kvadrat testi yordamida kiberstalkingga moyillikning ijtimoiy omillarga bog'liqligi baholandi.³

III.Natijalar

Bugungi kunda smartfon, ijtimoiy tarmoq profili yoki GPS funksiyasi yoqilgan qurilmaga ega bo'lgan har qanday odam kiber ta'qibning qurboniga aylanishi mumkin. Aslida, hozirda joylashuvni aniqlash texnologiyalari mavjud bo'lganligi sababli, kiber ta'qib odatiy ta'qibdan ko'ra keng tarqalgan. Shu sababli, ko'pchilik bunga ta'sirchan ekanligi sababli, ushbu tez o'sib borayotgan raqamli jinoyat haqida faktlarni o'rganish muhimdir.

Kiber ta'qibning jiddiyligini ko'rsatadigan ba'zi xavotirli statistik ma'lumotlar: har yili taxminan 7,5 million odam kiber ta'qibga duch keladi.⁴ Barcha ta'qib qurbonlarining 80 foizi texnologiya yordamida kuzatiladi, 67 foizi esa yuzma-yuz ta'qibga uchraydi va ba'zilar ikkala turdagi ta'qibga duch kelishadi. Ta'qib qurbonlarining 69 foizi katta darajada ruhiy zarba oladi.

Kiber ta'qib qurbonlari ko'pincha yuzma-yuz ta'qib qurbonlariga qaraganda ko'proq qo'rquvni boshdan kechiradi.⁵ Amerikaliklarning har 10 nafaridan 1 nafari shaxsiy GPS qurilmasi ruxsatsiz kuzatilgan yoki buzilgan.⁶ Kiber ta'qibchilarning 61 foizi smartfonlar, matnli xabarlar va elektron pochta kabi kundalik vositalardan foydalanadi, taxminan 10 foizi esa qurbonlarining hisoblariga kirish uchun zararli dasturlar yoki fishing texnikalaridan foydalanadi.⁷ Bakalavr talabalarning 41 foizigacha kiber ta'qibga duch kelgan.⁸ Yoshi 18 dan 24 yoshgacha bo'lgan kiber ta'qib qurbonlarining 16 foizi ta'qibchilar ular ruxsatisiz ularning jinsiy tusdagi fotosurat yoki videolarini tarqatganini aytishgan.⁹ Shuningdek, 2010 yildan 2020 yilgacha AQShning okrug sudlarida 412 ta federal kiber ta'qib ishi ochilgan.

Ushbu holatlarda ta'qibchilar qurbonlarini kuzatish uchun turli texnologiyalardan foydalangan, ammo eng ko'p ishlatilgan usullar matnli xabarlar, qo'ng'iroqlar va elektron pochta orqali bog'lanish bo'lgan. Ushbu ta'qib holatlarining deyarli yarmida ta'qibchilar qurbonlarini kuzatish uchun kameralar va ekran tasvirlarini olish usullaridan foydalanganlar.¹⁰

³ <https://Safehome.org> survey of 1,025 Americans (2023)

⁴ Brian Fitzpatrick United States Representative. (2024). Protecting Americans from Cyberstalking.

⁵ Smith, Sharon G. et al. (2022, Apr). The National Intimate Partner and Sexual Violence Survey:

⁶ Hemenway, Chad. (2023, Aug 23). Tile, Amazon Face Lawsuit From Stalking Victims Over Tracking Device Product. Insurance Journal.

⁷ Adamson, David M. et al. (2023). Cyberstalking: A Growing Challenge for the U.S. Legal System.

⁸ . Reyns, Bradford W. et al. (2011, Dec 5). Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students. Taylor & Francis Online.

⁹ SPARC (Stalking Prevention, Awareness, and Resource Center). (2024). Stalking & Technology.

¹⁰ Stevens, Francesca et al. (2021, Jun 14). Cyber Stalking, Syber Harassment, and Adult Mental Health: A Systematic Review. Mary Ann Liebert, Inc.

Qo'llangan texnologiyalar	Ko'rsatkichi
Matnli xabarlar, email, telefon yoki mobil tekefon	61%
Multimedia, masalan, kameralar, fotosuratlar va ekran tasvirlari	49%
Ijtimoiy tarmoq platformalari	43%
Shifrlash, anonim aloqa	16%
Xakerlik, masalan, fishing va zararli dasturlar	10%
Kuzatish, masalan, GPS va kalit yozuvchilar (keyloggerlar)	10%

Manba: Cyberstalking: A Growing Challenge for the U.S. Legal System, RAND Institute, 2023

Bugungi kunda kiber ta'qib odatiy (yuzma-yuz) ta'qibga qaraganda keng tarqalgan. AQSh Adliya Statistika Byurosi (BJS) ma'lumotlariga ko'ra, faqat 2019-yilda AQShda 16 yosh va undan katta bo'lgan taxminan 1,5 million odam (taxminan aholining 0,6 foizi) kiber ta'qib qurboniga aylangan. BJS hisobotiga ko'ra: Barcha ta'qib qurbonlarining taxminan 80 foizi kiber ta'qibga (yoki texnologik ta'qibga) duch kelgan bo'lsa, 67 foizi an'anaviy ta'qibga duch kelgan. Ko'pgina qurbonlar ikkala turdagi ta'qibga duch kelgan. Ayollar erkaklarga qaraganda ikki baravar ko'proq ta'qibga uchrigan. Taxminan 1,8 foiz ayollar ta'qibga uchrigan, erkaklar orasida bu ko'rsatkich bir foizdan past bo'lgan. Shuningdek, ushbu BJS hisobotiga ko'ra, barcha ta'qib qurbonlarining 67 foizi o'z ta'qibchisini tanigan va ko'pincha bu shaxs hozirgi yoki sobiq yaqin sherigi bo'lgan.

Yaqin sheriklar faqat bitta usulni emas, balki kiber va yuzma-yuz ta'qib usullarini birgalikda qo'llashga ko'proq moyil bo'lgan.¹¹

IV. Muhokama

Kimlar kiber-tahdidlarga uchrashi mumkin?

Olib borilgan tadqiqot natijalari shuni ko'rsatadiki, ayollar erkaklarga qaraganda kiber-tahdidlarga ko'proq duch keladi: Hayotining bir qismida uch kishidan biri ayollar va olti kishidan biri erkaklar kiber yoki jismoniy ta'qibga duch kelishadi.¹² Huquqni muhofaza qilish organlari ayrim guruhlar kiber-tahdidlarga yuqori darajada duch kelishini tushuntiradi.

¹¹ Morgan, Rachel E. and Jennifer L. Truman, Ph.D. (2022, Feb). Stalking Victimization, 2019. U.S. Department of Justice.

¹² Adamson, David M. et al. (2023). Cyberstalking: A Growing Challenge for the U.S. Legal System.

Ular orasida ayollar, LGBTQ insonlari, nogironlar, yoshlar va immigrantlar bor. Ular bir nechta sabablarga ko'ra, nishonga aylanib qolishadi, jumladan, ta'qibni xabar qilishlari kamroq bo'lishi mumkin deb hisoblanadi. Masalan, ta'qibchi kimnidir "gay" sifatida oshkor qilish bilan tahdid qilishi mumkin va jabrlanuvchi bu oshkor qilishdan qochib, jim turishi mumkin deb o'ylaydi. Kiber-ta'qib qurboni bo'lgan rangli irq'larga mansub odamlar ilgari huquqni muhofaza qilish organlari bilan yomon tajribalar tufayli politsiyaga murojaat qilishga qarshi bo'lishi mumkin.

Immigrantlar esa til to'siqlari yoki kamsitilishdan qo'rqishlari sababli kiber-tahdidlarga duch kelganliklarini xabar qilishda qiyinchiliklarga duch kelishadi.

Kiberstalking klassifikatsiyasi

Quyidagi xatti-harakatlarni kiberstalking sifatida tasniflash mumkin:

Takroran qo'ng'iroq qilish yoki xabar yuborish, noqulay elektron pochta, ijtimoiy tarmoqlardagi aloqa yoki xabarlarini yuborish, telefon qo'ng'iroqlari, kompyuterdan foydalanish yoki ijtimoiy tarmoq faoliyatini shaxsiy dasturiy ta'minot yoki boshqa vositalar orqali kuzatish, yashirin texnologiyalarni, masalan, kameralar yoki GPS texnologiyasini ishlatib, joylashuvlarni kuzatish, ijtimoiy tarmoq postlarini kuzatish yoki joylashuvlarni kuzatib boruvchi hisoblar yoki ilovalarni (masalan, taksi chaqirish ilovalari) buzib kirish orqali joylashuvlarni aniqlash, noqulay, istalmagan yoki shaxsiy ma'lumotlarni internetda yoki xabarlar orqali joylashtirish (yoki joylashtirish bilan tahdid qilish), onlayn mish-mishlarni tarqatish yoki boshqalarni jabrlanuvchini ta'qib qilishga undash.

V. Xulosa

Yuqoridagi tadqiqot shuni ko'rsatadiki, kiber-tahdidlarga uchragan jabrlanuvchilarning aksariyati o'z tajribalari haqida huquqni muhofaza qilish organlariga xabar bermaydi, buning eng keng tarqalgan sababi, ular o'z tajribalari jinoyat ekanligini bilmasliklari ekan. Ushbu ikkita asosiy topilmani hal qilish uchun ikki yo'nalishli yondashuv qo'llanilishi kerak.

Birinchi qadam — kiber-tahdidlarga uchraganlarni xabar berish darajasini oshirishga e'tibor qaratish. Ayollar va boshqa jinsiy identifikatsiya egalari (erkaklarga nisbatan) ko'proq "politsiya hech narsa qilmasligini o'ylashgan" deb, kiber-tahdidlari haqida xabar bermaganliklarini izohlagan, ammo boshqa jins yoki irq'lar bo'yicha farqlar kuzatilmagan. Shunday qilib, keng jamoatchilikka yo'naltirilgan ta'lim va xabardorlik dasturlari xabar berishni oshirishning samarali usuli bo'lishi mumkin.

Ushbu dasturlarda, kiber-tahdidlarga nima kirishi va jinoyat adliya tizimi javoblarini olish uchun qanday qadamlar tashlash kerakligini o'rgatish muhimdir. kinchi qadam — kiber-tahdidlarga oid voqea xabar berilganidan so'ng, jinoyat adliya tizimining javobini yaxshilashdir.

Stalking va kiber-stalking holatlari jinoyat adliya tizimi tomonidan sezilarli darajada kam qayd etiladi — bu kiber-tahdidlarga nisbatan ongning yo'qligi va yoki ularni aniqlash va tergov qilish ko'nikmalarining yetishmasligi, yurisdiksiya va qonuniy cheklovlar, va onlayn dalillarni olishdagi qiyinchiliklar sababli. Shunday qilib, huquqni muhofaza qilish organlari kiber-tahdidlarga oid ishlarni to'g'ri qayta ishlash uchun zarur resurslarga ega bo'lishi kerak.

Politsiyaning kiber-tahdidlarga oid xabar berilgan ishlarni amalga oshirmasligi, jabrlanuvchilarning kelajakdagi jabrlanishlar haqida xabar berishdan voz kechishiga sabab bo'lishi mumkin va jabrlanuvchining xavfsizligini xavf ostiga qo'yishi mumkin. Qisqacha aytganda, bu topilmalar kiber-tahdidlarga uchragan jabrlanuvchilarni huquqni muhofaza qilish organlariga xabar berishga rag'batlantirish uchun katta ishlarni amalga oshirish kerakligini ko'rsatadi, shunda ular o'z zararli tajribalardan tiklanish uchun zarur resurslarni olishi va jinoyatchilar o'z xatti-harakatlari uchun javobgar bo'lishi mumkin.

REFERENCES

1. Saydivalieva, K. K. (2022). The Role of Family Contracts in the Regulation of Family Relations and Their Juridical Nature. *International Journal of Social Science Research and Review*, 5(12), 553
2. MacFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour cyberspace: Towards a typology of cyberstalkers.
2. Alexis A. Moore "Cyberstalking and Women - Facts and Statistics"
3. Citron, D. K. (2009). Law's expressive value in combating cyber gender harassment.