TERGOV HARAKATLARINI O‘TKAZISHDA RAQAMLI TEXNOLOGIYALARDAN FOYDALANISHNING SAMARADORLIGI

Mirzakarimova Dilafruz Doniyorovna
Farg‘ona davlat universiteti
Maxsus huquqiy fanlar kafedrasi o‘qituvchisi

Annotatsiya: Ushbu maqolada raqamli asrda kiberxavfsizlikning muhim masalalari, kiberhujumlar chastotasi va murakkabligi muhim ahamiyatga ega. Kiberxavfsizlik tahdidlarini bartaraf etishdagi asosiy muammolardan biri yurisdiksiya chegaralari masalasidir, chunki kiberjinoyatchilar dunyoning istalgan nuqtasidan faoliyat yuritishi mumkin, bu esa huquqni muhofaza qilish organlariga ularni kuzatish va jinoiy javobgarlikka tortishni qiyinlashtiradi. Kibermakonning raqamli tabiati yurisdiksiyani aniqlashda o‘ziga xos muammolarni keltirib chiqaradi, chunki onlayn faoliyat jismoniy chegaralar va an’anaviy huquqiy asoslardan oshib ketishi mumkin. Ushbu tadqiqot ishida raqamli sohada yurisdiksiya chegaralarini aniqlash bilan bog‘liq nazariy masalalar hamda rivojlanayotgan landshaftni shakllantiradigan huquqiy, siyosiy va amaliy mulohazalar o‘rganilib, muhim takliflar ishlab chiqildi.

Kalit so’zlar: kiberxavfsizlik, kibermakon, axborot xavfsizligi, raqamli muhit, internet boshqaruvi, kiberxavf, kiberhujum, kiberjinoyat, ekstraterritorial yurisdiksiya, kiberhuquq, raqamli dalil.

EFFECTIVENESS OF USE OF DIGITAL TECHNOLOGIES IN INVESTIGATION

Abstract: This article highlights the critical issues of cyber security in the digital age, the frequency and sophistication of cyber attacks. One of the main challenges in addressing cyber security threats is the issue of jurisdictional boundaries, as cybercriminals can operate from anywhere in the world, making it difficult for law enforcement agencies to track and prosecute them. The digital nature of cyberspace creates unique jurisdictional challenges because online activity can transcend physical boundaries and traditional legal frameworks. This research paper examines the theoretical issues related to the definition of jurisdictional boundaries in the digital sphere, as well as the legal, political and practical considerations that shape the evolving landscape, and develops important proposals.

Key words: cyber security, cyber space, information security, digital environment, internet governance, cyber risk, cyber attack, cyber crime, extraterritorial jurisdiction, cyber law, digital evidence.

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИЯХ

Аннотация: В данной статье освещаются критические проблемы кибербезопасности в эпоху цифровых технологий, частота и сложность кибератак. Одной из основных проблем в борьбе с угрозами кибербезопасности является проблема границ юрисдикции, поскольку киберпреступники могут действовать из любой точки мира, что затрудняет их отслеживание и преследование правоохранительными органами. Цифровая природа киберпространства создает уникальные юрисдикционные проблемы, поскольку онлайн-деятельность может выходить за пределы физических границ и традиционных правовых рамок. В данной исследовательской работе рассматриваются теоретические вопросы, связанные с определением границ юрисдикции в цифровой сфере, а также юридические, политические и практические соображения, которые формируют развивающуюся ситуацию, и разрабатываются важные предложения.

Ключевые слова: кибербезопасность, киберпространство, информационная безопасность, цифровая среда, управление Интернетом, киберриск, кибератака, киберпреступность, экстерриториальная юрисдикция, киберправо, цифровые доказательства.

I.Kirish

Axborot almashishning yaxshilanishi mamlakatlar chegaralar bo‘ylab kibertahdidlar bo‘yicha razvedka ma’lumotlarini tobora ko‘proq almashishmoqda, bu esa kiberhujumlarni aniqlash va ularga javob berishda yanada samarali hamkorlik qilish imkonini beradi. Ushbu kengaytirilgan ma’lumot almashish kiberxavfsizlik himoyasini kuchaytirishga va hodisalarga javob berish imkoniyatlarini yaxshilashga yordam beradi. Ko‘pgina mamlakatlar paydo bo‘layotgan kibertahdidlarga javob berish va kiberjinoyatchilikka qarshi kurashda transchegaraviy hamkorlikni osonlashtirish uchun kiberxavfsizlik qonun-qoidalarini yanada takomillashtirmoqda. [1]

Kiberhujumlarni bartaraf etish uchun aniq huquqiy asoslarni yaratish orqali mamlakatlar kiberjinoyatchilarni ularning noqonuniy xatti-harakatlarini javobgarlikka torta olishadi. Raqamlashgan dunyoda raqamli ma’lumotlar sifatida ko‘plab xavfsiz ma’lumotlarni o‘z ichiga oladi, ular asosan internetda joylashtiriladi, uzatiladi va foydalaniladi. Muammo shundaki, kibermakonda qaysi qonunlar va qoidalar qo‘llanilishini aniqlash qiyin, chunki unda real dunyoning jismoniy chegaralari mavjud bo‘lmaydi. Kibermakon esa o‘ziga xos xususiyatga ega, chunki u onlayn faoliyat natijasida yaratilgan virtual makondir. [2]

Milliy qonunlarning xilma-xilligi va raqamli dunyoning ahamiyati ortib borayotganini hisobga olsak, kibermakonni qanday tartibga solish bo‘yicha global konsensus bo‘lishi aniq emas. Biroq, onlayn faoliyat uchun umume’tirof etilgan ba’zi ko‘rsatmalar mavjudBu jinoyatga qaysi davlat qonunlari amal qilishini aniqlashni qiyinlashtiradi. [3]

II.Metodologiya

Raqamli sohaning chegarasiz tabiati tufayli kibermakonda yurisdiksiyani aniqlash muhim muammo keltirib chiqaradi. Internetning markazlashtirilmagan tuzilishi va transchegaraviy aloqa va tranzaksiyalarning qulayligi ma’lum bir kibermakonda sodir etilgan jinoyatlar qaysi yurisdiksiya vakolatiga ega ekanligini aniqlashni murakkablashtiradi.

Kibermakonda yurisdiksiyaning umume’tirof etilgan asoslarini yaratish murakkab vazifa bo‘lib, xalqaro hamkorlikni, qonunlarni uyg‘unlashtirishni va raqamli sohani samarali boshqarishni ta’minlash uchun innovatsion yondashuvlarni talab qiladi. Yurisdiksiyaning an’anaviy konsepsiyasi, xususan, yurisdiksiyaning hududiy asosi asrlar davomida dunyo miqyosidagi huquqiy tizimlarning asosi bo‘lib kelgan. [4]

An’anaviy yurisdiksiya me’yorlari kiberfaoliyatning transmilliy tabiatiga moslashish uchun kurash olib boradi, bu esa yurisdiksiya bo‘shlig‘iga va potensial mojarolarga olib keladi. Birinchidan, internet jismoniy va yuridik shaxslarga jismoniy chegaralardan oshib ketadigan faoliyat bilan shug‘ullanish imkonini beradi, bu esa yurisdiksiya joyini aniqlashni qiyinlashtiradi. Ikkinchidan, raqamli tranzaksiyalar ko‘pincha bir nechta yurisdiksiyalarni o‘z ichiga oladi, bu esa qaysi qonunlar qo‘llanilishi kerakligi haqida chalkashlik va nizolarga olib keladi. Uchinchidan, kibermakon tomonidan taqdim etilgan tezlik va anonimlik an’anaviy hokimiyat organlarining samarali tergov va ijro harakatlariga to‘sqinlik qilishi mumkin. [5]

Nihoyat, Internetning global tabiati kibermakondagi yurisdiksiyaviy muammolarni hal qilish uchun xalqaro hamkorlik va qonunlarni uyg‘unlashtirish zarurligini anglatadi. Raqamli asrda kiberjinoyatlarning kuchayishi huquq tizimiga, xususan, Xalqaro xususiy huquq va shaxsiy daxlsizlik qonuni sohalarida jiddiy muammolarni keltirib chiqardi. Yurisdiksiya masalalari, qonunlarning ijro etilishi va xorijiy sud qarorlarining qo‘llanilishi muhim muammolarga aylandi, chunki kiberjinoyatlar milliy chegaralardan oshib, butun dunyo bo‘ylab shaxslar va tashkilotlarga ta’sir qildi. [6]

III.Natijalar

Yurisdiksiya chegaralari kiberxavfsizlik choralarini qo‘llash va kiberjinoyatlarni ta’qib qilishda qiyinchiliklar tug‘diradi. Bir yurisdiksiyada faoliyat yurituvchi aybdorlar javobgarlikdan qochish uchun xalqaro hamkorlik yoki qonunchilik asoslari yo‘qligidan foydalanishlari mumkin. Yurisdiksiya chegaralari ham ma’lumotlarni himoya qilish va maxfiylik qoidalarini ko‘rib chiqishda muhim rol

o‘ynaydi. Global miqyosda faoliyat yurituvchi kompaniyalar har bir yurisdiksiyada ma’lumotlarni himoya qilish bo‘yicha turli qonunlarga rioya qilishlari lozim. [7]

Kibermakonning jismoniy chegaralari yo‘qligi sababli, kiberxavfsizlik muammolarini hal qilish uchun samarali global boshqaruv mexanizmlarini o‘rnatish zaruratga aylanadi. Birlashgan Millatlar Tashkiloti va mintaqaviy kibertashkilotlar kabi xalqaro tashkilotlar kiberxavfsizlik normalari va protokollari bo‘yicha muhokamalar va kelishuvlarga ko‘maklashishda muhim rol o‘ynaydi. [8]

Raqamli landshaft rivojlanishda davom etar ekan, kibermakondagi yurisdiksiyaviy muammolarni hal qilish xavfsiz va ishonchlikibermuhitni rivojlantirish uchun hal qiluvchi ahamiyatga ega bo‘ladi. Yurisdiksiya chegaralari kibermakondagi ma’lumotlarni himoya qilish va maxfiylik qoidalariga katta ta’sir ko‘rsatadi. Samarali kiberxavfsizlik davlatlar o‘rtasida mustahkam transchegaraviy hamkorlikni talab qiladi. [9]

Xalqaro hamkorlikning ilg‘or tajribalari va institutsional mexanizmlarini tahlil qilish hamda global miqyosda kibertahdidlar va kiberjinoyatlarga qarshi samarali kurashish uchun yurisdiksiya chegaralarini kesib o‘tish zaruratini ta’kidlaydi. Bulutli hisoblash texnologiyalarining paydo bo‘lishi ma’lumotlar suvereniteti va yurisdiksiya chegaralari bilan bog‘liq muammolarni kuchaytirdi. [10]

IV. Muhokama qismi

Hududiy yurisdiksiyaning tarixiy rivojlanishini suverenitet tamoyillari va Vestfaliya tizimidan kuzatish mumkin, bu esa milliy davlatlarning o‘zlarining belgilangan hududlaridagi mutlaq hokimiyatini ta’kidladi. Bu tushuncha turli huquqiy doktrinalar va xalqaro shartnomalarda o‘z ifodasini topib, davlat o‘z chegaralarida yuzaga keladigan masalalarni tartibga solish va hal qilish huquqiga ega degan tushunchani mustahkamlaydi. [11]

Birinchidan, internet jismoniy va yuridik shaxslarga jismoniy chegaralardan oshib ketadigan faoliyat bilan shug‘ullanish imkonini beradi, bu esa yurisdiksiya joyini aniqlashni qiyinlashtiradi. Ikkinchidan, raqamli tranzaksiyalar ko‘pincha bir nechta yurisdiksiyalarni o‘z ichiga oladi, bu esa qaysi qonunlar qo‘llanilishi kerakligi haqida chalkashlik va nizolarga olib keladi. Uchinchidan, kibermakon tomonidan taqdim etilgan tezlik va anonimlik an’anaviy hokimiyat organlarining samarali tergov va ijro harakatlariga to‘sqinlik qilishi mumkin. [13]

Qiyosiy tahlil shuni ko‘rsatadiki, Amerika Qo‘shma Shtatlari, Kanada, Hindiston va Shveytsariya kiberxavfsizlik va kibermakonda yurisdiksiyani aniqlashda turlicha yondashuvlarni qo‘llagan. Amerika Qo‘shma Shtatlari va Kanadada onlayn faoliyatni boshqarish uchun yaxshi o‘rnatilgan qonunchilik asoslari va tartibga solish mexanizmlari mavjud bo‘lsa-da, Hindiston va Shveytsariya kiberxavfsizlikni boshqarishni kuchaytirish zarurligini ko‘proq tan olishmoqda. [14]

V.Xulosa

Raqamlashtirish va axborotning erkin oqimi global dunyoni o‘zgartirdi. Biroq, imkoniyatlarning ortishi bilan yangi va ortib borayotgan xavf-xatarlar, shuningdek, yurisdiksiya bo‘yicha sezilarli darajada farqlanishi mumkin bo‘lgan va doimiy ravishda rivojlanib boradigan murakkab qonunchilik rejimlari paydo bo‘ldi. Hatto, eng ishonchli kompaniya ham mijoz yoki kompaniya ma’lumotlarini o‘g‘irlash yoki to‘lov dasturi hujumi kabi kiberxavfsizlik hodisasining qurboni bo‘lishi mumkin. Biz ko‘plab transmilliy kompaniyalar bilan ularning kiberxavfsizlik xatarlarini boshqarish, tezkor javob rejalarini ishlab chiqish, kiberxavfsizlikni boshqarish bo‘yicha maslahatlarni taqdim etish va yuzaga kelishi mumkin bo‘lgan har qanday huquqiy muammolarni hal qilish uchun mijozlar bilan ommaviy so‘rovnomalar olib boriladi. [15]

Xulosa qilib aytganda, O‘zbekistonda kiberxavfsizlik va yurisdiksiyaga oidqonun hujjatlarini yaratish tizimli va kompleks yondashuvni talab qiladi. Ushbu asosiy qadamlarga rioya qilish va butun jarayon davomida manfaatdor tomonlar bilan hamkorlik qilish orqali kibertahdidlarga samarali javob beruvchi hamda O‘zbekistonning raqamli infratuzilmasini himoya qiluvchi qonunchilikni ishlab chiqish muhim hisoblanadi.

Foydalanilgan manbalar/Литература/References

1. “Kiberxavfsizlik asoslari”, A.A.Ganiev, S.K.Ganiev, Z.T.Xudoyqulov, Toshkent.: - 2020 B.8;
2. “Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar” N.S.Salaev, R.N.Ro‘ziev, Toshkent.: – 2018 b.23.
3. Smith, J. (2020). The Impact of Jurisdictional Boundaries on Cyber Security.
4. Journal of Cyber Security, 15(2), 123-137
5. Johnson, A. (2019). International Cooperation in Combating Cyber Crime.
6. International Journal of Law and Technology, 8(4), 301-315;
7. Cyber Security and Jurisdictional Boundaries: A Global Perspective. Retrieved from https://www.unodc.org/cybersecurity/;
8. Brown, M. (2018). Cyber Security Challenges in the Digital Age. Cybersecurity Journal, 12(3), 45-58;
9. World Economic Forum. (2020). Global Risks Report: Cyber Security Threats. Retrieved from https://www.weforum.org/global-risks-report;
10. National Institute of Standards and Technology. (2019). Cyber Security Framework for Critical Infrastructure Protection. NIST Special Publication 800-53;
11. European Union Agency for Cybersecurity. (2021). Annual Report on Cyber Security Trends. Retrieved from https://www.enisa.europa.eu/publications;
12. Ponemon Institute. (2019). Cost of Data Breach Study: Global Analysis. Retrieved from https://www.ibm.com/security/data-breach;
13. International Telecommunication Union. (2020). Global Cybersecurity Index: Country Rankings. Retrieved from https://www.itu.int/en/ITUD/Cybersecurity/Pages/GCI;
14. Cybersecurity and Infrastructure Security Agency. (2021). Cyber Security
15. Best Practices Guide. Retrieved from https://www.cisa.gov/cybersecurity-best practices;
16. Kiberxavfsizlik, raqamli huquq va hisob gigiyena –Kiberjinoyatchilikka qarshi muqobil yechim. Javlon Zoilboyev. 2022 yil avgust Obshchestvo va innovatsii 3(6/S):12-24 DOI: 10.47689/2181-1415-vol3-iss6/Spp12- LitsenziyaCC BY 4.0See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/362407860;
17. Henriksen, A. (2019). The End of the Road for the UN GGE Process: The
18. Future Regulation of Cyberspace. Journal of Cybersecurity, 5(1). DOI:https://doi.org/10.1093/cybsec/tyy009;
19. K. Ganimozhi and Aswathy Rajan, A study and Analysis of the Cyberspace
20. with special Reference to Jurisdictional Issues and Challenges, INTERNATIONAL
21. JOURNAL OF PURE AND APPLIED CYBERSECURITY.