

**KIBERHUJUMLAR VA SIYOSIY XAVF: DAVLATLAR O'RTASIDAGI
KIBER URUHLARNING IJTIMOIIY VA SIYOSIY TA'SIRI**

Abdurahmonov Zafar Botirovich

*Bojxona instituti, Axborot texnologiyalari va matematika kafedrası, katta o'qituvchi,
tel: +998909630306, Email: ucell@mail.ru*

Kenjayev Ibratbek Bahodir o'g'li

*Bojxona instituti, Bojxona ishi fakulteti, 2-kurs YuP-123 guruh kursanti, tel:
+998940045644, email: ibratjonkenjayev09@gmail.com*

Annotatsiya: *Zamonaviy dunyomizda internet va texnologiyalar hayotning ko'p qismini boshqaradigan bir paytda, davlatlar o'rtasidagi kiber urushlar tobora ko'payib bormoqda. Ko'pincha xakerlik vositalari yoki kiberxavfsizlik dasturlari kabi texnik jihatlarga ko'proq e'tibor qaratilsa-da, chuqurroq ijtimoiy va siyosiy oqibatlar ham jiddiy ahamiyatga ega. Ushbu maqolada kiberhujumlarning siyosiy beqarorlikka olib kelishi, jamoatchilik ishonchiga ta'siri va odamlarning kundalik hayotiga qanday ta'sir qilishi o'rganiladi. So'nggi ilmiy adabiyotlar va oxirgi bir necha yillik misollar asosida, maqolada hukumatlarning bu vaziyatga qanday munosabat bildirishi va xalqaro hamkorlikning kelajakda qanday rol o'ynashi mumkinligi ham muhokama qilinadi.*

Kalit so'zlar: *kiberurush, siyosiy xavf, jamiyat, xalqaro xavfsizlik, davlatlararo mojaró*

**КИБЕРАТАКИ И ПОЛИТИЧЕСКИЕ УГРОЗЫ: СОЦИАЛЬНОЕ И
ПОЛИТИЧЕСКОЕ ВОЗДЕЙСТВИЕ КИБЕРВОЙН МЕЖДУ
ГОСУДАРСТВАМИ**

Абдурахмонов Зафар Ботирович

*старший преподаватель кафедры информационных технологий и математики
Таможенного института, тел: +998909630306, Email: ucell@mail.ru*

Кенжаев Ибрatбек Баходир угли

*курсant 2-го курса факультета таможенного дела Таможенного института,
группа ЮП-123, тел: +998940045644, email: ibratjonkenjayev09@gmail.com*

Аннотация: *В современном мире, где интернет и технологии контролируют значительную часть жизни, кибервойны между государствами становятся все более распространенными. Хотя часто больше внимания уделяется техническим аспектам, таким как хакерские инструменты или программы кибербезопасности, более глубокие социальные и политические последствия также имеют серьезное значение. В этой статье рассматривается, как кибератаки приводят к политической нестабильности, влияют на общественное доверие и повседневную*

жизнь людей. На основе последней научной литературы и примеров за последние несколько лет, в статье также обсуждается, как правительства могут реагировать на эту ситуацию и какую роль может сыграть международное сотрудничество в будущем.

Ключевые слова: кибервойна, политическая угроза, общество, международная безопасность, межгосударственный конфликт

CYBERATTACKS AND POLITICAL THREAT: THE SOCIAL AND POLITICAL IMPACT OF CYBERWARS BETWEEN STATES

Abdurakhmanov Zafar Botirovich

Senior Lecturer, Department of Information Technologies and Mathematics, Customs Institute, tel: +998909630306, Email: ucell@mail.ru

Kenjayev Ibratbek Bakhodir ugli

cadet of group YuP-123 2nd year, Faculty of Customs Affairs, Customs Institute, tel: +998940045644, email: ibratjonkenjayev09@gmail.com

Abstract: *In our modern world, where the internet and technology govern many aspects of life, cyber warfare between states is becoming increasingly prevalent. While more attention is often focused on technical aspects such as hacking tools or cybersecurity programs, the deeper social and political implications are also of significant importance. This article examines how cyberattacks lead to political instability, their impact on public trust, and how they affect people's daily lives. Based on recent scientific literature and examples from the past few years, the article also discusses how governments might respond to this situation and what role international cooperation could play in the future.*

Keywords: *cyber warfare, political risk, society, international security, interstate conflict*

Kirish

So'nggi yillarda kibertexnologiyalar global siyosiy jarayonlarda tobora markaziy o'rinni egallamoqda. Mamlakatlar o'rtasidagi an'anaviy mojarolar bir paytlar harbiy kuchga tayangan, ammo bugungi kunda raqamli vositalar ko'pincha boshqa davlatning ichki tartibini buzish yoki unga qarshi chiqish uchun ishlatiladi. Kiberhujumlar endi masofadan turib aralashish - jismoniy hujumsiz zarar yetkazish imkonini beradi. Muhimi, bunday hujumlar AT tizimlaridan ancha uzoqqa borib yetadi va dastlab yashirin qolishi mumkin bo'lgan murakkab ijtimoiy va siyosiy oqibatlarni keltirib chiqaradi (Ahmedov, 2022)[1].

Dunyo bo'ylab sodir bo'lgan ko'plab hodisalar ushbu kibertahdidlarning ko'lami va jiddiyligini ko'rsatdi. Turli mamlakatlarda hukumat tizimlari, sog'ligni saqlash

muassasalari va moliyaviy tarmoqlar muvofiqlashtirilgan raqamli hujumlarga uchradi. Bu voqealar shunchaki texnik nosozliklar emas, balki kundalik hayotga ham ta'sir qiladi. Onlayn ovoz berish platformalaridagi uzilishlar yoki favqulodda vaziyat paytida shifoxona dasturiy ta'minotining o'chirilishi aholining xavfsizlik hissi va milliy yetakchilikka bo'lgan ishonchiga tezda putur yetkazishi mumkin. Demokratik institutlarga bo'lgan ishonchga putur yetganda, siyosiy xavf kuchliroq va uzoqroq davom etadi.

Usullar

Bu xavflarni tushunish uchun faqat texnik statistika yoki dasturlash modellariga qarash yetarli emas. Aksincha, mazkur tadqiqot 2018-2024 yillar oralig'ida chop etilgan adabiyotlar, mutaxassislar tahlili va amaliy misollarga asoslangan keng qamrovli sharhga tayanadi. Manbalar JSTOR, Scopus va Google Scholar kabi akademik ma'lumotlar bazalaridan ijtimoiy fanlar va xalqaro munosabatlarga urg'u berilgan holda to'plangan. Taxminan 25 ta ilmiy va siyosatga oid manbalar tanlab olingan. Asosiy e'tibor kiber hodisalarning hajmi yoki qiymatini o'lchashdan ko'ra, ularning mohiyatini anglashga qaratilgan. Ushbu usul empirik fan talablariga to'liq javob bermasa-da, u Markaziy Osiyo akademik tadqiqotlarida ko'p qo'llaniladigan insonparvarlik yondashuvini aks ettiradi.

Natijalar va muhokama

Ko'plab ilmiy tadqiqotlarda keltirilgan asosiy xulosa shuki, kiberhujumning oqibatlarini ko'pincha texnik jihatdan emas, balki psixologik va siyosiy jihatdan kuchliroq bo'ladi (Deibert, 2020)[2]. Hujum haqida e'lon qilingach, tizimlar tez tiklansa-da, zaiflik hissi odatda saqlanib qoladi. Fuqarolar tegishli himoya mavjudligiga shubha qila boshlaydilar. Agar hukumat bunday tahdidlarga qarshi kurashishga tayyor emasdek ko'rinsa, siyosiy ishonch pasayadi va jamoatchilik bosimi kuchayadi. Bir marta yo'qotilgan ishonchni qayta tiklash oson kechmaydi.

Zamonaviy kiberhujumlar ko'pincha ma'lumotni yo'q qilish yoki o'g'irlashgagina emas, balki jamoatchilik fikrini shakllantirish va idrokka ta'sir o'tkazishga ham qaratilgan. Bu ayniqsa ijtimoiy tarmoqlardagi dezinformatsiya kampaniyalari orqali amalga oshiriladi. Misol uchun, saylov davrlarida internetda muvofiqlashtirilgan raqamli harakatlar paydo bo'lib, saylovchilarni chalg'itish, soxta axborotni tarqatish yoki muxolifat ovozini bo'g'ishga urinadi. Bunday operatsiyalarning maqsadi har doim ham biror siyosiy kuchning g'alaba qozonishini ta'minlash emas; ba'zida asl niyat jamiyatda beqarorlik yoki bo'linish yaratishdan iborat bo'ladi. Bo'linishlar kuchaygan sari, ichki birlik zaiflashadi va mamlakat tashqi ta'sirga ko'proq beriluvchan bo'lib qoladi.

Kiberxavfsizlikning asosiy muammolaridan biri atribut muammosidir. Tanklar yoki raketalar kim javobgarligini aniq ko'rsatadigan an'anaviy urushdan farqli o'laroq, raqamli hujumlarni kuzatish qiyin (Carr, 2020)[3]. Ko'pgina tajovuzkorlar o'z shaxsini yashirish yoki boshqa birov mas'ul ekanligini ko'rsatish uchun usullardan foydalanadilar. Mojarolarning bu "kulrang zonasi" huquqiy va diplomatik javoblarni murakkablashtiradi. Hukumatlar to'liq dalillarsiz harakat qilishdan ikkilanishlari mumkin. Ba'zi hollarda,

jamoatchilik ayblovlari to'liq aniqlik kiritilmasdan amalga oshiriladi, bu esa xalqaro miqyosda ko'proq keskinlik yoki chalkashlikni keltirib chiqarishi mumkin. Keskinlashuvdan qo'rqish ko'plab mamlakatlarga ochiq javob berishga to'sqinlik qiladi, bu esa o'z navbatida aholining rasmiy javoblarga bo'lgan ishonchini pasaytiradi.

Kiberurush bo'yicha muhokamalar xalqaro hamkorlik masalasini ham o'z ichiga oladi. Nazariy jihatdan, ko'plab mamlakatlar global kiberqoidalar va umumiy xavfsizlik g'oyasini qo'llab-quvvatlaydi (ISRS, 2022). Biroq, amalda davlatlar o'rtasidagi ishonch ko'pincha haqiqiy hamkorlikka imkon berish uchun juda zaif bo'ladi (Zhora, 2023)[4]. Birlashgan Millatlar Tashkiloti yoki mintaqaviy muloqot platformalari kabi tashabbuslar ba'zi ko'rsatmalarni yaratdi, ammo ularning bajarilishi pastligicha qolmoqda. Kiber hokimiyat hali ham ko'pincha umumiy mas'uliyat emas, balki raqobat vositasi sifatida qaraladi. Kuchli hamkorlik bo'lmasa, raqamli tahdidlar to'xtovsiz o'sishda davom etadi.

Jamiyat nuqtayi nazaridan kiber hodisalarga munosabat odatda hissiy va tez bo'ladi (Healey, 2022)[5]. Katta raqamli hujumdan so'ng ko'plab fuqarolar ijtimoiy tarmoqlarga murojaat qilib, g'azab, qo'rquv yoki sarosima bilan o'rtoqlashadilar. Bu ko'pincha mish-mishlar yoki yolg'on hikoyalarning tarqalishiga olib keladi, ayniqsa hokimiyatdan aniq xabar bo'lmasa. Bu yerda hukumat kommunikatsiyasining roli juda muhim bo'ladi. Sekin yoki noaniq javob ishonchsizlikni oshirishi mumkin, o'z vaqtida va ochiq tushuntirish esa qo'rquvni tinchlantirishi va ijtimoiy hamjihatlikni himoya qilishi mumkin. Shunday qilib, kommunikatsiya siyosati kiberxavfsizlik strategiyasining muhim qismidir.

Jamoatchilik xabardorligi va ta'lim ham asosiy rol o'ynaydi. Aholi kiberxavfsizlikning asosiy tamoyillarini tushunadigan va noto'g'ri ma'lumotlarni aniqlay oladigan joylarda kiberoperatsiyalardan kelib chiqadigan umumiy siyosiy xavf kamayadi. O'zbekistonda va shunga o'xshash sharoitlarda ushbu sohadagi jamoatchilik bilimlari hali ham rivojlanmoqda. Biroq, oldinga siljish bor. Ta'lim muassasalarida kiberxavfsizlikni o'quv dasturlariga kiritish boshlanmoqda va raqamli xabardorlik dasturlari sekinlik bilan kengaymoqda. Bu qadamlar raqamli vositalar orqali boshqarish qiyinroq bo'lgan barqaror jamiyat qurish uchun juda muhimdir (Karimova, 2023)[6].

Xulosa

Xulosa qilib aytganda, kiberurush raqamli yoki texnik tahdiddan ko'ra ko'proq narsani anglatadi - u siyosiy tizimlar va ijtimoiy ishonch uchun jiddiy xavf tug'diradi. Kiberhujumlar asosiy xizmatlarni nishonga olish, fikrlarga ta'sir o'tkazish va noaniqliklarni tarqatish orqali milliy barqarorlikka putur yetkazadi. Hukumatlar nafaqat kuchli raqamli infratuzilmaga sarmoya kiritishi, balki mas'uliyatli muloqot, xalqaro hamkorlik va jamoatchilik xabardorligi uchun asos yaratishi kerak. Kibermojarolar murakkab va ko'pincha ko'rinmas bo'lib qolsa-da, ularning ta'siri haqiqiy va uzoq davom etadi. Xatarlarni kamaytirish siyosiy, texnik va ijtimoiy darajalarda keng ko'lamli sa'y-harakatlarni talab qiladi.

Adabiyotlar ro'yxati

1. Axmedov, I. M. (2022). Raqamli xavfsizlik siyosatining dolzarb muammolari va istiqbollari. O'zbekiston Respublikasi Fanlar Akademiyasi Axborot Texnologiyalari Instituti Ilmiy To'plami, 2(45), 67–74.
 2. Deibert, R. (2020). Reset: Reclaiming the Internet for Civil Society. House of Anansi.
 3. Carr, M. (2020). Cybersecurity and Global Politics: International Approaches to Cybercrime. Routledge.
 4. Zhora, V. (2023). Cyberattacks as the First Strike: Ukraine's Experience in Digital Warfare. Foreign Affairs, 102(3), 57–67.
 5. Healey, J. (2022). The Evolution of Cyber Conflict: Preparing for the Future. Journal of International Affairs, 75(2), 14–29.
 6. Karimova, Z. T. (2023). Kiberxavfsizlik sohasida davlat siyosatining shakllanishi: xalqaro tajriba va O'zbekiston misolida. Jahon siyosati va xavfsizlik muammolari, 1(19), 14–26.
- O'zbekiston Respublikasi Prezidenti huzuridagi Strategik va mintaqalararo tadqiqotlar instituti. (2022). Kiberxavfsizlik va raqamli suverenitet: zamonaviy tahdidlar va O'zbekiston tajribasi. <https://isrs.uz>