AXBOROT URUSHLARINING SHAKLLARI

Muallif: ***Zaidov Azizbek Avazbekovich***
O‘zbekiston Respublikasi Jamoat Xavfsizligi
Universiteti magistratura tinglovchisi, podpolkovnik

Annotatsiya

Maqolada axborot urushlarining asosiy shakllari — psixologik ta’sir, kiberhujumlar, kiberpropaganda, media manipulyatsiya va dezinformatsiya hamda ijtimoiy tarmoqlar orqali ta’sir usullari tahlil etilib, ularni inson ongiga ta’sir o‘tkazishda, siyosiy jarayonlarni boshqarishda va milliy xavfsizlikni izdan chiqarishda qo‘llash mumkin bo‘lgan vositasi sifatida ko‘rib chiqilgan. Shuningdek, O‘zbekiston qonunchiligida axborot xavfsizligi sohasidagi me’yoriy asoslar va xalqaro tajribaga asoslangan tavsiyalar keltirilgan.

Kalit so‘zlar: axborot urushi, axborot xavfsizligi, kiberhujum, dezinformatsiya, media manipulyatsiya, milliy xavfsizlik, ijtimoiy tarmoqlar, kiberpropaganda.

Аннотация

В статье анализируются основные формы информационных войн — психологическое воздействие, кибератаки, кибропропаганда, медиа-манипуляции и дезинформация, а также методы воздействия через социальные сети. Эти формы рассматриваются как инструменты, которые могут использоваться для влияния на сознание людей, управления политическими процессами и подрыва национальной безопасности. Кроме того, в статье представлены нормативные основы в области информационной безопасности в законодательстве Узбекистана и рекомендации, основанные на международном опыте.

Ключевые слова: информационная война, информационная безопасность, кибератака, дезинформация, медийная манипуляция, национальная безопасность, социальные сети, киберпропаганда.

Abstract

The article analyzes the main forms of information warfare — psychological influence, cyberattacks, cyber propaganda, media manipulation, and disinformation, as well as methods of influence through social networks. These forms are considered as tools that can be used to affect human consciousness, manage political processes, and undermine national security. In addition, the article presents the regulatory framework for information security in Uzbekistan’s legislation and recommendations based on international experience.

Keywords: information warfare, information security, cyberattack, disinformation, media manipulation, national security, social networks, cyber propaganda.

Kirish

XXI asrda axborot jamiyati shakllanishi va raqamli texnologiyalarning jadal rivojlanishi global munosabatlarning barcha sohalariga jiddiy ta’sir ko‘rsatdi. Axborot endi faqat ma’lumot almashinuv vositasi emas, balki siyosiy, iqtisodiy va harbiy kurashning strategik quroliga aylandi. Shu jarayonda “axborot urushi” tushunchasi ilmiy va amaliyot sohalarida alohida ahamiyat kasb etmoqda.

Bunday urushlar ko‘p hollarda harbiy harakatlarsiz, ya’ni “noan’anaviy front”da amalga oshiriladi.

Zamonaviy axborot urushlarining o‘ziga xos jihati shundaki, ular ochiq mojarolar orqali emas, balki internet makonidagi media resurslar, ijtimoiy tarmoqlar, feyk axborot va kiberhujumlar orqali olib boriladi. Bu esa nafaqat davlatlar, balki har qanday fuqaro yoki tashkilotni ham axborot ta’siri obyektlari qatoriga qo‘yadi.

Dunyo miqyosida axborot urushlari 1990-yillardan boshlab yangi bosqichga ko‘tarildi. AQSh va NATOning harbiy doktrinalarida “information warfare”, “psychological operations”, “cyber operations” kabi atamalar davlat strategiyalarining muhim qismi sifatida mustahkam o‘rin egalladi. Rossiya, Xitoy, Eron kabi davlatlar ham o‘z navbatida axborot maydonida raqobatbardosh imkoniyatlar yaratmoqda.

O‘zbekiston uchun bu mavzu alohida ahamiyatga ega, chunki axborot xavfsizligi milliy xavfsizlikning uzviy qismi hisoblanadi. Mamlakatda raqamli iqtisodiyotni rivojlantirish, axborot-kommunikatsiya tizimlarini modernizatsiya qilish bilan birga, tashqi axborot ta’sirlariga qarshi samarali tizim yaratish ham muhim vazifa hisoblanadi.

Mazkur maqolada axborot urushlarining asosiy shakllari va vositalari tahlil qilinib, ayrim takliflar milliy xavfsizlik nuqtai nazaridan ularning oqibatlari va O‘zbekiston tajribasidagi qonunchilik asoslari yoritiladi.

Axborot urushlarining asosiy shakllari va vositalari.

Axborot urushlari tushunchasi ilmiy muomalaga XX asrning ikkinchi yarmidan kirib kelgan bo‘lib, u avvalo harbiy strategiya, siyosiy psixologiya va kommunikatsiya nazariyasi sohalarida qo‘llanila boshlangan. Bu atamaning turli ta’riflari mavjud bo‘lib, ular umumiy jihatdan bir g‘oyaga — axborotning siyosiy va harbiy ta’sir vositasi sifatida qo‘llanilishiga borib taqaladi.

Amerikalik tadqiqotchi M.Libitskiy (M.Libicki) ta’kidlaganidek, axborot urushi — bu “inson ongi va axborot tizimlari ustidan nazorat uchun kurash”dir.

Axborot urushlari hozirgi zamonaviy geosiyosiy muhitda davlatlar va nodavlat subyektlar o‘rtasidagi raqobatning asosiy vositasiga aylandi. Ular harbiy

to‘qnashuvlarsiz ham siyosiy ta’sir, iqtisodiy bosim yoki ijtimoiy beqarorlikni keltirib chiqarish imkonini berib, turli shakllarda namoyon bo‘ladi.

Quyida axborot urushlarining asosiy shakllari va ularda qo‘llaniladigan vositalar tahlil qilinadi.

1. Psixologik axborot ta’siri.

Axborot urushlarining ildizi psixologik ta’sir texnologiyalariga borib taqaladi. Bu shakldagi urushlarda asosiy maqsad — jamoatchilik ongini ma’lum yo‘nalishda o‘zgartirish, hissiyotlarga ta’sir ko‘rsatish va jamiyatda notinchlik yoki ishonchsizlik muhitini shakllantirishdir.

Psixologik axborot ta’siri ko‘pincha “qo‘rqitish”, “ishontirish” yoki “umid uyg‘otish” mexanizmlari orqali amalga oshiriladi. Masalan, ma’lum davlat yoki siyosiy kuch haqida salbiy axborotni tizimli ravishda tarqatish natijasida jamoatchilikda manfiy obraz hosil qilinadi.

Bu jarayonda ***kognitiv psixologiya*** (inson ongining fikrlash, xotira, qaror qabul qilish, e’tibor va ma’lumotni qayta ishlash), ***PR texnologiyalari*** (tashkilot yoki shaxsning obro‘sini oshirish, auditoriya bilan ijobiy munosabatlar o‘rnatish va axborot oqimini boshqarish usullari) va ***neyromarketing*** (inson miyasining reklama va marketingga reaksiyasi) usullaridan foydalaniladi. Axborot ta’sirining samarasi jamiyatning axborot savodxonligi darajasiga, ommaviy axborot vositalariga bo‘lgan ishonchga va siyosiy muhitga bog‘liq.

Psixologik axborot urushining misollaridan biri sifatida 2003-yildagi Iroq urushi oldidan ommaviy axborot vositalari orqali tarqatilgan “ommaviy qirg‘in qurollari” haqidagi dezinfomatsiyani ko‘rsatish mumkin. Bu axborot AQSh jamoatchiligini harbiy amaliyotni qo‘llab-quvvatlashga moyil qilib, siyosiy qaror qabul qilish jarayoniga ta’sir ko‘rsatgan.

Psixologik axborot ta’sirining asosiy bosqichlari quyidagicha:

- auditoriyaning ruhiy holatini o‘rganish;
- ta’sir strategiyasini ishlab chiqish;
- axborot kanallarini tanlash (TV, internet, ijtimoiy tarmoqlar va h.k.);
- hissiy yondoshuv orqali fikr shakllantirish;
- ta’sir natijalarini tahlil qilish va qayta ishlov berish.

2. Kiberhujumlar va kiberpropaganda.

Kiberhujumlar - axborot urushlarining texnik shakliga kiradi va ular raqib davlatning axborot infratuzilmasiga zarar yetkazish, ma’lumot oqimini buzish yoki maxfiy ma’lumotlarni o‘g‘irlash orqali amalga oshiriladi.

Kiberhujumlar quyidagi ko‘rinishlarda bo‘ladi:

- **DDoS (Distributed Denial of Service)** — server yoki veb-saytlarni ortiqcha trafik bilan to‘ldirish orqali ishlamay qolishiga sabab bo‘lish;

- **Phishing** — foydalanuvchilarni aldov orqali shaxsiy ma’lumotlarini oshkor qilishga majbur qilish;
- **Malware** — zararli dasturlar orqali axborot tizimlariga kirish va ularni boshqarish;
- **Defacing** — veb-saytning tashqi ko‘rinishi yoki kontentini o‘zgartirish orqali psixologik ta’sir ko‘rsatish.

Kiberhujumlar ko‘pincha kiberpropaganda bilan uyg‘un holda amalga oshiriladi.

Kiberpropaganda — bu internet va raqamli media orqali ma’lum siyosiy yoki mafkuraviy g‘oyalarni ommaviy ravishda tarqatish, raqib haqida salbiy axborot oqimini yuritish jarayonidir.

Masalan, 2016-yildagi AQSh prezidentlik saylovlari davomida kiberpropaganda orqali feyk axborot tarqatish, ijtimoiy tarmoqlarda avtomatik botlar orqali fikrlarni manipulyatsiya qilish holatlari qayd etilgan.

Shu sababdan kiberxavfsizlik nafaqat texnik muammo, balki siyosiy strategiyaning muhim qismiga aylandi. Davlatlar kiberhujumlarga qarshi kurashish uchun maxsus agentliklar tashkil etmoqda (masalan, AQShda — “Cyber Command” – Kiber qo’mondonlik, Rossiyada — “Войска информационных операций” –Axborot operatsiyalari qo‘shinlari, Xitoyda — “Network Defense Unit” – Tarmoqni himoya qilish bo‘limi).

3. Media manipulyatsiya va dezinfomatsiya.

Media manipulyatsiya axborot urushlarining eng keng tarqalgan shakli hisoblanadi. Uning mohiyati — ommaviy axborot vositalari orqali ma’lum voqea, shaxs yoki davlat haqidagi ma’lumotni bir tomonlama yoritish, kontekstni burish, faktlarni yashirish yoki buzib ko‘rsatishdan iborat.

Dezinfomatsiya esa — haqiqatga to‘g‘ri kelmaydigan ma’lumotlarni ongli ravishda tarqatish jarayonidir. Buning orqali jamiyatda ishonchsizlik, xavotir, yolg‘on tasavvurlar paydo boladi.

Media manipulyatsiya vositalari quyidagilardan iborat:

- axborotni **freyming** orqali (ya’ni ma’lum kun tartibini belgilash) yo‘naltirish;
- **ommaviy obraz** yaratish (masalan, dushman yoki qurbon sifatida ko‘rsatish);
- ma’lumotni **burmalash** (aslda bo‘lmagan voqealarni uydirish yoki mavjud faktlarni o‘zgartirish);
- **tasviriy va audio vositalar** orqali hissiy ta’sir (qo‘rquv, nafrat yoki rahmdillik uyg‘otish).

Media manipulyatsiyaning ilg‘or shaklidan biri - “feyk axborot fabrikalari”ning faoliyatidir. Ular avtomatik botlar yordamida ijtimoiy tarmoqlarda ma’lum pozitsiyani ommalashtiradi va jamoatchilik fikrini sun’iy ravishda yaratadi.

Dezinfomatsiyaning yana bir turi — **deepfake** texnologiyalari. Unda sun’iy intellekt yordamida odam ovozi va videosi qalbakilashtiriladi, natijada haqiqiyga o‘xshash, ammo soxta kontent yaratiladi. Bu texnologiya axborot urushlarining yangi bosqichini boshladi.

4. Ijtimoiy tarmoqlar orqali ta’sir usullari.

Ijtimoiy tarmoqlar XXI asrda axborot urushlarining asosiy maydoniga aylandi. Ularning afzalligi — ma’lumotning tez tarqalishi, keng qamrovli auditoriya va shaxsiylashtirilgan ta’sir imkoniyatlaridir.

Axborot urushlarida ijtimoiy tarmoqlardan quyidagi yo‘llar bilan foydalaniladi:

- **Feyk akkauntlar** yaratish va ular orqali ma’lum siyosiy yoki ideologik g‘oyalarni targ‘ib qilish;
- **Bot tarmoqlari** orqali ma’lum xeshtag yoki fikrni ommalashtirish;
- **Target reklama** orqali ma’lum guruhlarning ongini yo‘naltirish;
- **Kontent** orqali hissiy ta’sir ko‘rsatish (masalan, shoklovchi tasvirlar, video yoki shov-shuvli xabarlar).

Ijtimoiy tarmoqlardagi axborot urushlari ko‘pincha “kognitiv bosim” orqali amalga oshiriladi, ya’ni insonning fikrlash tizimiga ma’lum doirada ta’sir qilinadi. Masalan, ma’lum siyosiy voqea haqida doimiy ravishda bir xil yo‘nalishdagi axborot tarqatish orqali jamoatchilik ongida “haqiqat illuziyasi” yaratiladi.

Bugungi kunda Facebook, X (sobiq Twitter), Telegram, TikTok va boshqa platformalar axborot urushlarining asosiy instrumentlariga aylandi. Shuning uchun davlatlar va jamiyat axborot immunitetini kuchaytirish — ya’ni feyk va manipulyatsiyaga qarshi turish qobiliyatini rivojlantirishni ustuvor vazifa qilib belgilamoqda.

Xulosa.

Axborot urushlari turli shakllarda (psixologik, kiber, media va ijtimoiy platformalar orqali) amalga oshirilishi, ularning maqsadi, jamoat ongi va axborot muhitini nazorat qilishga qaratilganligi hamda harbiy kuch yoki iqtisodiy salohiyatdan ham ustun bo‘lishi mumkinligi, global va milliy xavfsizlikka sezilarli tahdid bo‘lib qolayotganligini inobatga olib, O‘zbekistonda qonunchilik va milliy strategiyalarni rivojlantirish orqali axborot xavfsizligini mustahkamlashi, uning turli shakllarida xavfsizlikni va zamonaviy tahdidlarga samarali javob berishi hamda o‘z axborot xavfsizligini strategik darajada muhofaza qilishga intilishi zarur.

Shu boisdan, yuqoridagi masalalar yechimi yuzasidan ayrim takliflarni berib o‘tishni joiz deb o‘ylayman:

1. Milliy kiberxavfsizlik markazlari va monitoring tizimlarini modernizatsiya qilish va kiberhimoyani rivojlantirish.

2. Maktablarda, universitetlarda, yoshlar markazlarida axborot xavfsizligi va media savodxonlik kurslarini joriy etish shuningdek ommaviy axborot vositalari hamda ijtimoiy tarmoqlarda dezinformatsiyaga qarshi profilaktika tadbirlarini amalga oshirish.

3. Axborot urushlari va kiberhujumlarga qarshi mukammal qonunlar ishlab chiqish barobarida xususiy sektorning mas'uliyatini aniq belgilab berish.

4. Xalqaro standartlar va protokollar asosida tajriba almashishni keng yo'lga qo'yish hamda feyk axborot va kiber tahdidlarning global monitoring va tahlilida faol ishtirok etish.

Foydalanilgan adabiyotlar ro'yxati

1. Castells, M. (2011). *The Rise of the Network Society*. Wiley-Blackwell.
2. Nye, J. S. (2010). *Cyber Power*. Harvard University Press.
3. Freedman, L. (2016). *Strategy: A History*. Oxford University Press.
4. Bogdanov, K. (2018). *Informatsionnye voyny i sovremennye konflikty*. Moscow: Nauka.
5. NATO Cooperative Cyber Defence Centre of Excellence. (2020). *Cyber Defence and Information Operations*. Tallinn.
6. Government of the Republic of Uzbekistan. (2019). *National Strategy on Cybersecurity*. Tashkent.
7. Law of the Republic of Uzbekistan "On Information Security and Informatization". (2018). Tashkent.
8. Pomerantsev, P. (2014). *Nothing is True and Everything is Possible: Adventures in Modern Russia*. PublicAffairs.
9. European Commission. (2018). *Code of Practice on Disinformation*. Brussels.
10. West, D. M. (2018). *Air Wars: Television Advertising and Social Media in Election Campaigns, 2008–2016*. Brookings Institution Press.