



INFORMATION ATTACK PREVENTION: ANALYSIS OF COMPLICATIONS, STRATEGIES AND FUTURE PROSPECTS

Jakhongir E. Aliyev

Doctoral student

Tashkent State University of Oriental Studies

Tashkent, Uzbekistan

E-mail: aliyehongir2330@gmail.com

ABOUT ARTICLE

Key words: information war, information space, disinformation, intelligence war, information security.

Abstract: This author's article analyzes the global attack and its types, media, classification and methods of information warfare, and implementation mechanisms.

Received: 28.04.24

Accepted: 30.04.24

Published: 02.05.24

AXBOROT XURUJLARINI OLDINI OLISH: MURAKKABLIK, STRATEGIYALAR VA KELAJAK ISTIQBOLLARINI TAHLIL QILISH

Jaxongir E. Aliyev

Tayanch-doktorant

Toshkent davlat sharqshunoslik universiteti

Toshkent, O'zbekiston

E-mail: aliyehongir2330@gmail.com

MAQOLA HAQIDA

Kalit so'zlar: axborot urushi, axborot makonini, dezinformatsiya, razvedka urushi, axborot xavfsizligi.

Annotatsiya: Ushbu muallif tomonidan maqolada globallashtirilgan axborot makonida axborot xurujlari va ularning turlari, shuningdek, axborot urushining tasnifi va usullari hamda amalga oshirish mexanizmlari tahlil qilindi.

ПРЕДУПРЕЖДЕНИЕ ИНФОРМАЦИОННЫХ АТАК: АНАЛИЗ ОСЛОЖНЕНИЙ, СТРАТЕГИИ И ПЕРСПЕКТИВЫ НА БУДУЩЕЕ

Джахонгир Э. Алиев

Докторант

Ташкентский государственный университет востоковедения

Ташкент, Узбекистан

E-mail: aliyehongir2330@gmail.com

О СТАТЬЕ

Ключевые слова: информационная война, информационное пространство, дезинформация, разведывательная война, информационная безопасность.

Аннотация: В статье данного автора проанализированы информационная атака и ее виды в глобализованном информационном пространстве, а также классификация и методы информационной войны и механизмы реализации.

KIRISH

Axborot makonining vujudga kelishi nafaqat uni bo'lib olish, balki unda kechayotgan jarayonlarni nazorat qilish va boshqarishni hoxlovchi tomonlarning paydo bo'lishiga olib keldi. Bu guruhlarining kurash vositasi ham aynan axborot qurolidir. Tahlilchilar axborot quroli deganda odamlarga ruhiy ta'sir ko'rsatadigan va ularning ustidan nazorat qilish imkonini beruvchi vositalarni, davlat va harbiy sohalarni boshqarishda axborotlarni soxtalashtirish kabi harakatlarni nazarda tutishadi.

Axborot xavfsizligiga nisbatan tahdidlarning asosiy ta'sir vositasi bir martalik tashviqot aksiyalari, uzoq muddatli targ'ibot kompaniyalari, mafkuraviy tazyiq, madaniy ekspansiya, axborot blokadası kabi ruhiy-informatsion ta'sir vositalari hisoblanadi.

Ayni paytda, kishilik jamiyati rivojida ustuvor bo'lib borayotgan mayllardan kelib chiqiladigan bo'lsa, insoniyatning istiqbolini ham tasavvur qilish imkonini beradi. Internet va ijtimoiy tarmoqlar hukmron bo'lgan davrda dezinformatsiyaning tarqalishi global muammoga aylandi.

Ushbu jarayon yangi hodisa emas va tarix davomida siyosiy, mafkuraviy va strategik maqsadlarda foydalanilgan. Biroq, internet va ijtimoiy tarmoqlarning paydo bo'lishi dezinformatsiya manzarasini o'zgartirib, uning ta'siri va ta'sirini kuchaytirdi. Davlat ishtirokchilari, siyosiy faollar, ekstremistik guruhlar va turli kun tartibiga ega shaxslar global miqyosda dezinformatsion kampaniyalarni tashkil qilish uchun onlayn platformalarning ochiqqligi va anonimligidan foydalanadilar.

ASOSIY QISIM**1. Kelib chiqishi va motivi:*****Davlat aktarlari:***

- Geosiyosiy maqsadlar: Davlat ishtirokchilari o'zlarining geosiyosiy manfaatlarini ilgari surish uchun boshqa mamlakatlardagi saylovlar natijalariga ta'sir o'tkazish, raqib hukumatlarni beqarorlashtirish yoki jamoatchilik fikrini o'z foydasiga shakllantirish kabi dezinformatsion kampaniyalarda qatnashishi mumkin.

- Targ'ibot va idrokni boshqarish: Hukumatlar dezinformatsiyadan tashviqot va idrokni boshqarish vositasi sifatida foydalanadi, hokimiyat va nazoratni saqlab qolish uchun ham ichki, ham xalqaro miqyosda jamoatchilik fikrini manipulyatsiya qiladi.

- Gibril urush: Dezinformatsiya ko'pincha gibril urush strategiyalarining bir qismi sifatida qo'llaniladi, bunda davlatlar ochiq to'qnashuvlarga murojaat qilmasdan strategik maqsadlarga erishish uchun odatiy harbiy taktikalar, kiberooperatsiyalar va axborot urushi kombinatsiyasidan foydalanadilar.

Siyosiy partiyalar:

- Saylov ustunligi: Siyosiy partiyalar va nomzodlar raqiblarini obro'sizlantirish, saylovchilarning ishtirokini bostirish yoki ularning bazasini safarbar qilish orqali saylovda ustunlikka erishish uchun dezinformatsiya tarqatishi mumkin.

Ekstremistik guruhlar:

- Yollash va radikallashtirish: Ekstremistik tashkilotlar yangi a'zolarni jalb qilish, zaif shaxslarni radikallashtirish va ekstremistik mafkuralarni tarqatish uchun dezinformatsiyadan foydalanadilar.

- Zo'ravonlikni qo'zg'atish: Dezinformatsiyadan dushmanlarga qarshi zo'ravonlikni qo'zg'atish, nafrat va kamsitishni targ'ib qilish va terrorchilik harakatlarini oqlash uchun foydalanish mumkin.

2. Taktika va strategiyalar:

Kontent yaratish:

- Manipulatsiya qilingan ommaviy axborot vositalari: Dezinformatsion aktyorlar noto'g'ri ma'lumot yoki hodisalarni noto'g'ri ko'rsatish uchun tasvirlar, videolar, audio yozuvlar yoki boshqa multimedia kontentini yaratishi yoki o'zgartirishi mumkin. Bu tanlab tahrirlangan tasvirlar, kontekstdan tashqari raqamli o'zgartirilgan vizuallarni o'z ichiga olishi mumkin.

Strategik maqsadlilik:

- Demografik maqsadlilik: Dezinformatsion kampaniyalar siyosiy mansubligi, etnik kelib chiqishi, dini yoki ijtimoiy-iqtisodiy holati kabi omillarga asoslanib, muayyan demografik guruhlar, jamoalar yoki hududlarni strategik maqsad qilib qo'yishi mumkin. Kontentni ushbu guruhlar bilan rezonanslash uchun moslashtirish dezinformatsiya ishtirokchilariga mavjud zaifliklardan, tarafkashliklardan yoki shikoyatlardan foydalanish imkonini beradi.

- Hodisalarni o'g'irlash: dezinformatsion kampaniyalar noto'g'ri ma'lumotlarni tarqatish va jamoatchilik fikrini shakllantirish uchun saylovlar, tabiiy ofatlar yoki sog'liqni saqlash inqirozlari kabi yirik voqealardan foydalanishi mumkin.

Ushbu voqealar atrofidagi ma'lumotlarni o'g'irlash orqali dezinformatsion aktyorlar o'z xabarlarini kuchaytirishi va ommaviy nutqqa ta'sir qilishi mumkin.

Muvofiqlashtirish va hamkorlik:

- Tarmoqli kampaniyalar: Dezinformatsion kampaniyalar ko'pincha soxta ma'lumotlarni kuchaytirish va umumiy maqsadlarga erishish uchun muvofiqlashtirilgan tarmoqlar yoki alyanslarda birgalikda ishlaydigan bir nechta aktyorlarni o'z ichiga oladi. Ushbu tarmoqlarga davlat tomonidan homiylik qilinadigan tezkor xodimlar, siyosiy faollar, ommaviy axborot vositalari va onlayn ta'sir o'tkazuvchilar kirishi mumkin.

- Platformalararo integratsiya: Dezinformatsion kampaniyalar kengroq auditoriyani qamrab olish va xabar almashishni kuchaytirish uchun bir nechta onlayn platformalar va aloqa kanallarini birlashtirishi mumkin. Veb-saytlar, ijtimoiy media, xabar almashish ilovalari va boshqa onlayn forumlardan foydalanib, dezinformatsiya qiluvchilar uzluksiz va keng tarqalgan tashviqot ekotizimini yaratishi mumkin.

Dezinformatsiya kampaniyalarida qo'llaniladigan turli xil taktika va strategiyalarni tushunib, manfaatdor tomonlar ularning zararli ta'sirini yumshatish va ommaviy nutq va demokratik jarayonlarning yaxlitligini himoya qilish uchun yanada samarali qarshi choralar va javoblarni ishlab chiqishlari mumkin.

3. Jamiyatga ta'siri:

Ishonchning buzilishi:

- Dezinformatsiya institutlar, ekspertlar va an'anaviy OAV manbalariga bo'lgan ishonchni yo'qotib, demokratiya va fuqarolik faolligi asoslariga putur etkazadi.

- Shaxslar noto'g'ri yoki chalg'ituvchi ma'lumotlarga duchor bo'lganda, ular rasmiy axborot manbalariga shubha bilan qarashlari, hukumatga, ommaviy axborot vositalariga va boshqa nufuzli institutlarga bo'lgan ishonchning pasayishiga olib kelishi mumkin.

- Ishonch emirilishi umumiy noaniqlik, beadablik va befarqlik tuyg'usini keltirib chiqarishi mumkin, bu esa jamiyatni dolzarb muammolarni hal qilish va asosli qarorlar qabul qilishni qiyinlashtiradi.

Demokratik jarayonlarga putur yetkazish:

- dezinformatsiya saylovchilar xulq-atvoriga ta'sir ko'rsatish, saylovchilar ishtirokini bostirish yoki saylov natijalarini qonuniylashtirishga qaratilgan noto'g'ri yoki chalg'ituvchi ma'lumotlarni tarqatish orqali demokratik jarayonlar, jumladan, saylovlar yaxlitligiga putur etkazadi.

- Saylovlarning adolatligi va qonuniyligiga shubha uygʻotgan holda, dezinformatsiya aholining demokratik institutlarga boʻlgan ishonchini susaytiradi, vakillik boshqaruvi asoslarini buzadi.

4. Kelajakdagi muammolar va mulohazalar:

Texnologiyadagi yutuqlar:

- Deepfake Technology: Deepfake texnologiyasi rivojlanishda davom etar ekan, juda ishonarli soxta videolar va audioyozuvlarni yaratish yanada qulayroq va keng tarqalib ketishi mumkin. Deepfakes ta'sirini aniqlash va yumshatish texnologiya kompaniyalari, tadqiqotchilar va siyosatchilar uchun jiddiy muammolarni keltirib chiqaradi.

- AI tomonidan yaratilgan kontent: AI tomonidan yaratilgan kontentning, jumladan, matn, tasvir va videolarning koʻpayishi haqiqat va fantastika oʻrtasidagi chegarani yanada xiralashtirishi mumkin, bu esa haqiqiy va uydirma ma'lumotni farqlashni tobora qiyinlashtirmoqda. AI tomonidan yaratilgan dezinformatsiyaning tarqalishiga qarshi kurashish innovatsion yondashuvlar va texnologik echimlarni talab qiladi.

Globalashuv va transchegaraviy tahdidlar:

- Transmilliy dezinformatsiya tarmoqlari: Dezinformatsion kampaniyalar milliy chegaralardan borgan sari oshib bormoqda, davlat va nodavlat sub'ektlar yurisdiksiyalar boʻylab yolgʻon ma'lumotlarni tarqatish va butun dunyo boʻylab jamoatchilik fikriga ta'sir qilish uchun hamkorlik qilmoqda. Xalqaro javob choralari va hamkorlikni muvofiqlashtirish transmilliy dezinformatsiya tahdidlarini samarali hal qilish uchun muhim boʻladi.

- Demokratik davlatlarga xorijiy aralashuv: Xorijiy hukumatlar va dushman shaxslar dezinformatsiyalarni tarqatish, boʻlinuvchi ma'lumotlarni kuchaytirish va demokratik institutlarga ishonchni susaytirish orqali demokratik jarayonlarga, jumladan, saylovlarga aralashishda davom etishi mumkin. Demokratik barqarorlikni mustahkamlash va chet el aralashuviga qarshi turish hukumatlar, fuqarolik jamiyati va xususiy sektorning birgalikdagi sa'y-harakatlarini talab qiladi.

- Sogʻliqni saqlash inqirozlari vaqtida notoʻgʻri ma'lumotlar: Pandemiya kabi sogʻliqni saqlash inqirozlari notoʻgʻri ma'lumotlar va dezinformatsiyaga qarshi kurashda oʻziga xos muammolarni keltirib chiqaradi, chunki notoʻgʻri ma'lumotlar tez tarqalishi va hayot uchun xavfli oqibatlariga olib kelishi mumkin. Inqirozga qarshi samarali muloqot strategiyalarini ishlab chiqish, ilmiy savodxonlikni oshirish va nufuzli manbalarga ishonchni mustahkamlash sogʻliqni saqlashdagi favqulodda vaziyatlarda notoʻgʻri ma'lumotni bartaraf etish uchun muhim boʻladi.

5. Qarshi choralalar va javoblar:

Faktlarni tekshirish va tekshirish:

- Mustaqil Fact-Chekking Tashkilotlari: Fakt-tekshiruvchi tashkilotlar yolg'on ma'lumotni yo'q qilish va yangiliklar va kontentning to'g'riligini tekshirishda hal qiluvchi rol o'ynaydi. Ushbu tashkilotlar da'volarning to'g'riligini baholash, dalillarni tahlil qilish va jamoatchilikka to'g'ri ma'lumot berish uchun o'qitilgan jurnalist va tadqiqotchilarni jalb qiladi.

Tartibga solish choralari:

- Qonunchilik va me'yoriy-huquqiy hujjatlar: Hukumatlar dezinformatsiyani joylashtirish uchun onlayn platformalarni javobgarlikka tortish, siyosiy reklama uchun shaffoflik talablarini ta'minlash va yomon niyatli shaxslar uchun jazo choralari qo'llash bo'yicha qoidalarni amalga oshirishi mumkin. Tartibga solish choralari nafrat so'zlari, zo'ravonlikka undash va yolg'on ma'lumotlarning tarqalishiga qarshi qonunlarni o'z ichiga olishi mumkin.

- Platforma siyosati va kontentni moderatsiya qilish: Onlayn platformalar noto'g'ri yoki chalg'ituvchi kontentni taqiqlash, zararli ma'lumotlarga kirishni cheklash va qoidabuzar kontentni olib tashlash uchun kontentni moderatsiya qilish mexanizmlarini joriy qilish kabi dezinformatsiyaga qarshi kurash siyosati va yo'riqnomalarini qabul qilishi mumkin.

Mediasavodxonlik ta'limi:

- Tanqidiy fikrlash ko'nikmalari: Media savodxonligi va tanqidiy fikrlash ko'nikmalarini targ'ib qilish odamlarga yolg'on rivoyatlardan ishonchli ma'lumotlarni ajratib olish va dezinformatsiya kampaniyalarida qo'llaniladigan manipulyatsiya taktikasiga qarshi turish imkonini beradi. Ta'lim dasturlari talabalar va keng jamoatchilikka manbalarni qanday baholash, ma'lumotni tekshirish va targ'ibot usullarini aniqlashni o'rgatishi mumkin.

- Raqamli savodxonlik dasturlari: Raqamli savodxonlik dasturlari odamlarga raqamli landshaftda xavfsiz, mas'uliyatli va axloqiy tarzda harakat qilishlariga yordam beradigan treninglar va resurslarni taqdim etadi. Ushbu dasturlar onlayn maxfiylik, axborot gigienasi va raqamli fuqarolik kabi mavzularni qamrab olishi mumkin.

Texnologik yechimlar:

- Avtomatlashtirilgan aniqlash vositalari: Avtomatlashtirilgan aniqlash vositalari va algoritmlarini ishlab chiqish dezinformatsiyani real vaqtda aniqlash va belgilashga yordam beradi, bu esa tezroq javob berish va kontentni yanada samarali moderatsiya qilish imkonini beradi. Ushbu vositalar tarkibni ishonchliligi va ishonchliligi asosida tahlil qilish va tasniflash uchun mashinani o'rganish, tabiiy tilni qayta ishlash va boshqa AI usullaridan foydalanishi mumkin.

Xalqaro hamkorlik:

- Global hamkorlik: Dezinformatsiyaga qarshi kurashish hukumatlar, texnologik kompaniyalar, fuqarolik jamiyati tashkilotlari va xalqaro tashkilotlar o'rtasida global miqyosda

dezinformatsiyaga qarshi kurash bo'yicha umumiy standartlar, protokollar va strategiyalarni ishlab chiqish uchun muvofiqlashtirilgan sa'y-harakatlarni talab qiladi.

Global hamkorlik axborot almashish, salohiyatni oshirish va dezinformatsion tahdidlarga hamkorlikda javob berishni osonlashtirishi mumkin.

- Diplomatik hamkorlik: Diplomatik hamkorlik va ko'p tomonlama tashabbuslar dezinformatsiya maqsadlarida axborot va kommunikatsiya texnologiyalaridan noto'g'ri foydalanishning oldini olish bo'yicha me'yorlar, tamoyillar va kelishuvlarni ilgari surishi mumkin. Diplomatik sa'y-harakatlar konsensus o'rnatish, muloqotni rivojlantirish va dezinformatsiya bilan bog'liq umumiy muammolarni hal qilish uchun davlatlar o'rtasida hamkorlikni rivojlantirishga qaratilishi mumkin.

Ushbu qarshi choralar va javoblarni amalga oshirish orqali manfaatdor tomonlar dezinformatsiyaning zararli oqibatlarini yumshatish, ommaviy nutqning yaxlitligini himoya qilish va raqamli asrda demokratik qadriyatlarni qo'llab-quvvatlash uchun birgalikda ishlashi mumkin.

XULOSA

Xulosa qilib aytadigan bo'lsak, dezinformatsiyaning tarqalishi jamiyat, demokratiya va ommaviy nutq uchun jiddiy muammolarni keltirib chiqaradi. Soxta ma'lumotlardan tortib algoritmik manipulyatsiyagacha, dezinformatsion kampaniyalar raqamli ekotizimimizdagi zaifliklardan foydalanadi, ishonchni yo'qotadi, qutblanishni kuchaytiradi va ma'lumotlarning yaxlitligini buzadi. Biroq, dezinformatsiyaning ko'p qirrali mohiyatini va uning jamiyat hayotining turli jabhalariga ta'sirini tushunib, manfaatdor tomonlar uning zararli oqibatlariga qarshi kurashish uchun samarali strategiya va aralashuvlarni ishlab chiqishlari mumkin.

Faktlarni tekshirish tashabbuslari, tartibga solish choralari, media savodxonligi bo'yicha ta'lim va texnologik echimlar dezinformatsiyaga qarshi kurashda hal qiluvchi rol o'ynaydi. Tanqidiy fikrlash ko'nikmalarini targ'ib qilish, shaffoflik va mas'uliyatni oshirish hamda hukumatlar, texnologik kompaniyalar, fuqarolik jamiyati tashkilotlari va xalqaro tuzilmalar o'rtasida hamkorlikni rivojlantirish orqali biz dezinformatsiyaga qarshi chidamlilikni oshirishimiz hamda haqiqat, halollik va demokratik qadriyatlar tamoyillarini qo'llab-quvvatlashimiz mumkin.

Oldinga qarab, texnologiya taraqqiyoti, globallashtirish va axloqiy dilemmalar kabi paydo bo'ladigan muammolar va mulohazalarni oldindan bilish juda muhimdir. Hushyor bo'lish, yangi tahdidlarga moslashish va innovatsion yondashuvlarni qo'llash orqali biz rivojlanayotgan dezinformatsiya landshaftida ishonch va qat'iyat bilan harakat qilishimiz mumkin.

Oxir oqibat, dezinformatsiyaning asosiy sabablarini bartaraf etish jamiyatning barcha qatlamlaridan birgalikdagi sa'y-harakatlarni talab qiladi. Birgalikda ishlash orqali biz haqiqat yolg'ondan ustun bo'ladigan va axborot ekotizimimizda ishonch tiklanadigan yanada xabardor, bardoshli va demokratik raqamli kelajakni qurishimiz mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe report.
2. DiResta, R., Shaffer, K., Ruppel, J., & Sullivan, D. (2018). The Tactics & Tropes of the Internet Research Agency. New Knowledge report.
3. Guess, A., Nyhan, B., & Reifler, J. (2020). Exposure to untrustworthy websites in the 2016 US election. *Nature Human Behaviour*, 4(5), 472-480.
4. Pennycook, G., & Rand, D. G. (2020). Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proceedings of the National Academy of Sciences*, 117(6), 2997-3005.
5. European Commission. (2018). Code of Practice on Disinformation. Available at: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.
6. Brennen, J. S., Simon, F., Howard, P. N., & Nielsen, R. K. (2020). Types, sources, and claims of COVID-19 misinformation. Reuters Institute Report.
7. Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094-1096. [DOI: 10.1126/science.aao2998]
8. Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., & Quinn, S. C. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American Journal of Public Health*, 108(10), 1378-1384. [DOI: 10.2105/AJPH.2018.304567]
9. Bradshaw, S., & Howard, P. N. (2019). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Oxford Internet Institute report. [Available online: <https://comprop.oii.ox.ac.uk/research/cybertroops2019/>]
10. Chadwick, A., & Vaccari, C. (2019). News sharing on UK social media: Misinformation, disinformation, and correction. *Political Communication*, 36(1), 136-158. [DOI: 10.1080/10584609.2018.1486579]