ISSN: 2181-4341, IMPACT FACTOR (RESEARCH BIB) – 7,245, SJIF – 5,431

Shaxzodbek Ibragimov, Tumanboyeva Durdona
Namangan muhandislik-texnologiya instituti “Avtomatika va energetika” fakulteti talabalari

KIBER URUSH VA DAVLATLARARO KIBER HUJUMLAR

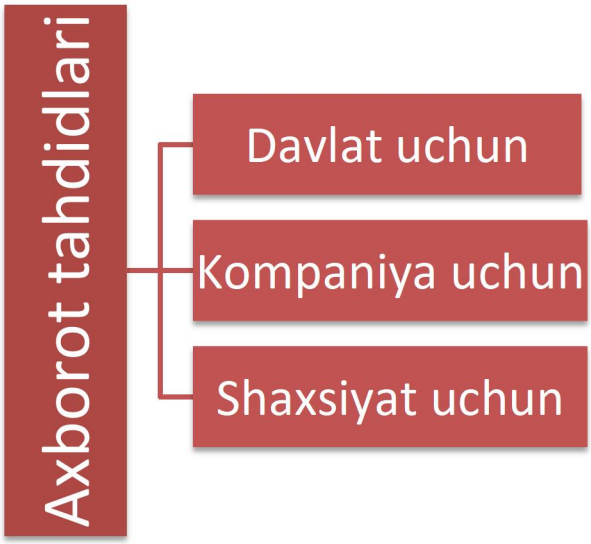
Annotatsiya: Ushbu maqola so‘nggi yillarda dolzarb bo‘lib borayotgan kiber urush va davlatlararo kiber hujumlar mavzusiga bag‘ishlangan. Unda kiber urushning mazmuni, asosiy maqsadlari va mashhur kiber hujumlar misollari tahlil qilinadi. Shuningdek, maqola kiberxavfsizlikni ta’minlash yo‘nalishida xalqaro hamkorlikning zaruriyati, davlatlarning strategik yondashuvlari va zamonaviy texnologik yechimlarni o‘z ichiga oladi. Kiber urushning xavflari va ularni bartaraf etish bo‘yicha amaliy tavsiyalar keltirilgan. Ushbu tadqiqot natijalari kiber xavfsizlikka oid xalqaro siyosat va davlatlararo munosabatlarni tartibga solishda muhim ahamiyatga ega bo‘lishi mumkin.

Ka’lit so’zlar: kiber urush, kiber hujumlar, kiberxavfsizlik, davlatlararo nizolar, texnologik innovatsiyalar, xalqaro hamkorlik, kiberjinoyatchilik, raqamli infratuzilma, kiber tahdidlar, axborot xavfsizligi.

Kirish

So‘nggi yillarda texnologiyalar va internet infratuzilmasining kengayishi bilan davlatlararo kiber urushlar va kiber hujumlar dolzarb masalaga aylandi. Kiber urush tushunchasi ko‘proq davlatlar orasida axborot texnologiyalari orqali olib boriladigan nizolarni anglatadi. Kiber hujumlar esa davlatlar yoki boshqa tashkilotlar tomonidan raqib davlatning muhim axborot tizimlari va infratuzilmasiga zarar yetkazish maqsadida amalga oshiriladigan harakatlar hisoblanadi. Mavzuning dolzarbligi bir necha omillarga bog‘liq. Birinchidan, davlatlar o‘rtasidagi raqobat va geosiyosiy ziddiyatlar yangi texnologiyalar orqali yangi urush maydonlarini yaratdi. Bu kiber urushlarning zamonaviy qurol sifatida faol qo‘llanilishiga olib keldi. Masalan, Rossiya va AQSh o‘rtasidagi kiber hujumlar, Shimoliy Koreyaning boshqa davlatlarga nisbatan amalga oshirgan hujumlari kabi misollar bu jarayonning kuchayib borayotganini ko‘rsatadi. Umuman olganda, kiber urush va kiber hujumlar mavzusi zamonaviy dunyoda davlatlararo nizolar va xavfsizlik masalalarining yangi ko‘rinishini aks ettiradi. Texnologik taraqqiyotning jadal sur’atlari bu mavzuni kelajakda ham dolzarb bo‘lib qolishini ta’minlaydi.

Bugungi kunda kiber xavfsizlik kundan kunga tobora rivojlanib borayotganligi va insonlar orasida ishonchsizlikni kuchaytiryotgani hech kimga sir emas. **Kiberxavfsizlik** – bu raqamli tizimlar, tarmoqlar, qurilmalar va ma'lumotlarni kiberhujumlardan, zararli dasturlardan, ruxsatsiz kirishlardan va boshqa kiberjinoyatlardan himoya qilish uchun amalga oshiriladigan chora-tadbirlar va texnologiyalar to‘plamidir. Kiberxavfsizlikning asosiy maqsadi axborotning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdir. “**Tahdid**” deganda u yoki bu tarzda axborot xavfsizligini buzishning potentsial imkoniyati tushuniladi. Tahdidni amalga oshirishga urinish “**hujum**”, bu urinishni amalga oshiruvchi esa “**hujumchi**” deb ataladi. Ko'pincha tahdid axborot tizimlarini himoya qilishda zaifliklarning mavjudligi natijasidir.



Yuqoridagilarni umumiy qiladigan bo'lsak bularni hammanisi mezoni kiber urish hisoblanadi.

Kiber urush – bu davlatlar yoki davlatlar bilan bog'liq bo'lgan tashkilotlar o'rtasida raqamli texnologiyalar yordamida amalga oshiriladigan hujumlar to'plami bo‘lib, u an'anaviy urushlardagi jangovar operatsiyalarga o'xshash tarzda amalga oshiriladi. Kiber urush davlatlar o'rtasidagi ziddiyatlarda muhim vositaga aylanmoqda, chunki u milliy xavfsizlikni, iqtisodiyotni va infratuzilmani bevosita tahdid ostiga qo'yadi. Bu turdagi hujumlar davlatlararo raqobat va strategik ustunlik uchun tobora keng qo'llanilmoqda.

Quyidagi omillar mavzuning dolzarbligini belgilaydi:

1. Kiber urushning maqsadlari:

- Harbiy infratuzilma va mudofaa tizimlari: Dushman davlatning harbiy infratuzilmasiga zarar yetkazish, radar tizimlarini, aloqa tarmoqlarini bloklash va qurollar boshqaruv tizimlarini ishdan chiqarish maqsadida hujumlar amalga oshirilishi mumkin.

- Energiya va transport tizimlari: Elektr energiyasi tarmoqlari, gaz va neft quvurlari, transport tizimlari kabi muhim infratuzilmalarni zaiflashtirish orqali davlatning barqarorligiga tahdid qilish.

- Ma'lumot va kommunikatsiya: Shpionlik va razvedka orqali maxfiy davlat yoki harbiy ma'lumotlarni qo'lga kiritish, raqib davlatning axborot tizimlarini izdan chiqarish, dezinformatsiya orqali ijtimoiy tanglik yaratish.

2. Mashhur kiber urush voqealari:

- Stuxnet (2009-2010): Isroil va AQSh tomonidan qo‘llab-quvvatlangan hujum bo‘lib, Eronning yadro infratuzilmasiga zarar yetkazish maqsadida ishlab chiqilgan zararli dastur. Bu kiber hujum natijasida Eronning Natanz yadro zavodi ishdan chiqqan.

- Estoniya (2007): Estoniyada 2007-yilda bo‘lib o‘tgan kiberhujumlar Rossiya bilan bog‘langan va hukumat saytlariga, banklar, ommaviy axborot vositalariga hujum qilingan. Bu kiberhujumlar davlat tizimlarini bir necha hafta davomida izdan chiqargan.

- Ukraina (2015-2016): Rossiya tomonidan qo'llab-quvvatlangan xakerlar Ukraina energiya tarmoqlariga zarar yetkazgan va bu oqibatda elektr energiyasi ta'minoti buzilgan. Bu hujumlar kiber urushning real dunyodagi infratuzilmaga bo'lgan jiddiy ta'sirini ko'rsatdi.

4. Davlatlararo kiber hujumlar:

- AQSh va Xitoy: Xitoyning davlat tomonidan qo'llab-quvvatlangan xaker guruhlari AQSh mudofaa va texnologiya sektorlari ma'lumotlarini o'g'irlashda ayblangan. Kiberhujumlar orqali AQSh korporatsiyalaridan sanoat sirlarini o'g'irlash, razvedka ma'lumotlarini yig'ish maqsad qilib qo'yilgan.

- Rossiya va G‘arb davlatlari: Rossiya NATO davlatlari va Yevropa Ittifoqiga nisbatan bir qator kiberhujumlar uyushtirganlikda ayblangan. 2016-yilda AQSh saylovlariga aralashish va bir qator Yevropa davlatlarida siyosiy jarayonlarga ta'sir ko‘rsatishga urinish bu misollardan biridir.

Yechimlar:

Kiber urush va davlatlararo kiber hujumlarni bartaraf etish jiddiy xalqaro muammolarni hal qilishda muhim ahamiyatga ega. Buning uchun davlatlar o‘z infratuzilmasini himoyalash, hujumlarga tezkor javob berish va xalqaro hamkorlikni mustahkamlash bo‘yicha ko‘plab yechimlarni qabul qilishlari kerak. Quyida kiber urush va kiber hujumlarni bartaraf etish bo‘yicha asosiy yechimlar keltirilgan:

1. Kiberxavfsizlik siyosatini kuchaytirish:

- Davlat darajasida kiberxavfsizlik strategiyasini ishlab chiqish: Har bir davlat o‘z kiberxavfsizlik strategiyasini ishlab chiqishi va muntazam yangilab turishi lozim. Bu strategiya hujumlarning oldini olish, zararni kamaytirish, va tezkor javob choralari bo‘yicha aniq rejalarni o‘z ichiga olishi kerak.

- Himoya infratuzilmasini mustahkamlash: Hukumat tashkilotlari, muhim infratuzilma tizimlari va moliyaviy institutlar kiber hujumlardan himoya qilish uchun o‘z tizimlarini doimiy ravishda yangilab turishlari lozim. Bu yerda firewall, antiviruslar, tarmoq monitoringi va himoyalangan tarmoq qoplamalari (VPN) muhim rol o‘ynaydi.

2. Kiber hujumlarni oldini olish uchun texnologik innovatsiyalar:

- Sun'iy intellekt va mashina o‘rganish: Kiber hujumlarni oldindan aniqlash va zararni kamaytirish uchun sun'iy intellekt va mashina o‘rganish texnologiyalaridan foydalanish kiber xavfsizlikning muhim qismiga aylanmoqda. Ushbu texnologiyalar hujumlar bo‘yicha ogohlantirishlar berish va avtomatik himoya qilish uchun ishlatiladi.

- Shifrlash va autentifikatsiya: Davlatlar o‘z tizimlaridagi ma'lumotlarni yanada ishonchli shifrlash texnologiyalari orqali himoya qilishlari kerak. Shuningdek, kuchli autentifikatsiya va ko'p faktorli identifikatsiya tizimlaridan foydalanish zarur.

3. Xalqaro hamkorlik va kelishuvlar:

- Xalqaro kelishuvlar: Kiber hujumlarni bartaraf etishda davlatlar o‘rtasidagi xalqaro kelishuvlar va qonuniy choralarning muhim roli bor. Davlatlar kiberjinoyatchilikni oldini olish va bunday hujumlar uchun javobgarlikni aniq belgilash uchun xalqaro darajada hamkorlik qilishlari

kerak. Masalan, BMT yoki NATO kabi tashkilotlar orqali kiberxavfsizlik bo‘yicha xalqaro qoidalar ishlab chiqilishi mumkin.

- Mutaxassislar va ma'lumot almashinuvi: Davlatlar o‘zaro kiberxavfsizlik mutaxassislari bilan hamkorlik qilish va tajriba almashish orqali kiber hujumlarga qarshi samarali choralar ko‘rishlari mumkin. Bu kiberhujumlar yuz berganda tezkor javob berishga imkon yaratadi.

4. Kiberjinoyatchilikni qonuniy tartibga solish va javobgarlik:

- Kiberjinoyatlarni xalqaro qonunlar bilan tartibga solish: Kiberjinoyatchilikni xalqaro miqyosda tartibga solish va bunday jinoyatlarni sodir etgan davlatlar yoki tashkilotlarni javobgarlikka tortish uchun global qonunchilik bazasi yaratish lozim. Bunda davlatlararo kiberhujumlar uchun jazolar va sanksiyalar aniq belgilanishi kerak.

- Huquqiy hamkorlik: Davlatlar kiberjinoyatchilikka qarshi kurashda birgalikda ishlashlari, kiberjinoyatchilarni aniqlash va ularni sudga tortish bo‘yicha hamkorlik qilishlari lozim.

5. Ijtimoiy ong va madaniyatni oshirish:

- Aholi orasida kiber savodxonlikni oshirish: Kiber urush va hujumlarga qarshi kurashda fuqarolarning xabardorligini oshirish muhim. Ommaviy axborot vositalari, ta'lim muassasalari va maxsus dasturlar orqali fuqarolarni kiberxavfsizlik qoidalariga rioya qilish va himoyalanish bo‘yicha o'rgatish zarur.

- Ommaviy axborot vositalarini nazorat qilish va dezinformatsiyaga qarshi kurash: Davlatlar kiber urush doirasida tarqaladigan noto‘g‘ri ma'lumotlar va dezinformatsiyaga qarshi kurashish uchun maxsus axborot monitoringi tizimlarini ishlab chiqishlari kerak.

Metodlar:

Mazkur maqolada kiber urush va kiber hujumlar bo‘yicha tarixiy voqealar, mavjud ma'lumotlar va misollar tahlil qilindi. Tadqiqot quyidagi usullar asosida amalga oshirildi:

1. **Hujjat tahlili**: Stuxnet, Estoniya va Ukraina hujumlari bo‘yicha ochiq manbalar va akademik maqolalar o‘rganildi.
2. **Sistematik yondashuv**: Davlatlar o‘rtasidagi kiber hujumlarning maqsadlari va oqibatlari tahlil qilinib, ularning kiber urushlardagi roli baholandi.
3. **Qiyosiy tahlil**: Turli davlatlar o‘rtasidagi kiber hujum strategiyalari va ular uchun qo‘llanilgan texnologik yechimlar solishtirildi.

Natijalar:

Tadqiqot natijalari kiber urushning quyidagi asosiy jihatlarini yoritadi:

1. **Kiber urushning maqsadlari**:
   - Harbiy infratuzilmaga hujum qilib, aloqa tizimlarini izdan chiqarish.
   - Energetika va transport tizimlariga zarar yetkazish orqali davlatning barqarorligiga tahdid qilish.
   - Ma'lumotlar o‘g‘irlash va dezinformatsiya orqali siyosiy tanglik yaratish.

2. **Kiber urushning mashhur misollari**:
   - **Stuxnet (2009-2010)**: Eronning yadro inshootlariga zarar yetkazish uchun ishlab chiqilgan zararli dastur.
   - **Estoniya (2007)**: Rossiya bilan bog‘liq bo‘lgan hujumlar natijasida Estoniya hukumat tizimlari bir necha hafta davomida ishlamay qoldi.
   - **Ukraina (2015-2016)**: Rossiya tomonidan qo‘llab-quvvatlangan hujumlar energiya ta'minotining buzilishiga olib keldi.
3. **Davlatlararo kiber hujumlar**:
   - Xitoyning AQSh texnologik sektori va mudofaa sohasiga nisbatan razvedka hujumlari.
   - Rossiyaning Yevropa va NATO davlatlariga qarshi amalga oshirgan kiber hujumlari.

Xulosa

Yuqoridagilardan kelib chiqqan holda, shuni aytish lozimki. Kiber urush va davlatlararo hujum zamonaviy davlatlar o'rtasidagi yangi jang maydoni bo‘lib, u raqamli texnologiyalarga tayanadi. Bu urushlarning maqsadi raqib davlatning harbiy, iqtisodiy, siyosiy va ijtimoiy tizimlariga zarar yetkazishdan iborat. Kiber urushda davlatlar o‘zaro kiber hujumlar orqali razvedka ma’lumotlarini qo‘lga kiritish, muhim infratuzilmalarga hujum qilish, siyosiy barqarorlikni buzish yoki iqtisodiy inqiroz keltirib chiqarishga intiladilar. Kiber urushning xavflari chuqur va keng qamrovli bo‘lib, milliy xavfsizlikka jiddiy tahdid soladi. Davlatlar raqamli texnologiyalarga bog‘liq bo‘lgani sababli, kiber hujumlar an'anaviy urushlardan ko‘ra tez va yashirin amalga oshiriladi.

Bartaraf etish yechimlari sifatida davlatlar kiberxavfsizlik strategiyalarini kuchaytirish, texnologik infratuzilmani himoya qilish, xalqaro hamkorlikni rivojlantirish, kiberxavfsizlik bo‘yicha qonunchilikni kuchaytirish va tezkor javob berish markazlarini tashkil etishlari zarur. Ushbu choralar kiberhujumlarni oldini olish va ularga tezkor javob berishga imkon beradi. Kiber urushning oldini olish va bartaraf etishda global miqyosda hamkorlik va xavfsizlikka oid umumiy qoidalarni ishlab chiqish zarur deb o’ylayman.

Foydalanilgan adabiyotlar

1. Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*. Simon & Schuster. (Kiber urush tarixi va mashhur hujumlar haqida umumiy ma'lumotlar uchun asosiy manba sifatida tavsiya etiladi.)
2. Stuxnet Case Study. (2010). *International Journal of Critical Infrastructure Protection*. (Eron yadro zavodlariga Stuxnet dasturi orqali amalga oshirilgan hujumlar haqida.)
3. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Analysis of Estonia Cyber Attacks 2007*. (Estoniya hukumat tizimlariga qilingan hujumlarni o'rganish bo'yicha xalqaro tadqiqotlar.)
4. Rid, T., & McBurney, P. (2012). *Cyber-Weapons*. RUSI Journal, 157(1), 6–13. (Kiber qurollarning rivojlanishi va ular qo'llanilishining tahlili.)
5. Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins. (Davlatlararo kiber urush tahdidlari va strategiyalari haqida.)
6. United Nations Office for Disarmament Affairs (UNODA). *Developments in the Field of Information and Telecommunications in the Context of International Security*. (BMTning kiberxavfsizlik bo'yicha xalqaro tashabbuslari va hamkorlikni rivojlantirish dasturlari.)
7. Kovacs, E. (2016). *Ukraine Cyberattack: Analysis of Russian-Backed Operation*. SecurityWeek. (Ukraina energetika tizimlariga hujum va uning oqibatlari bo'yicha tahlil.)