



GIBRID URUHLARNING NAZARIY ASOSLARI VA ZAMONAVIY XUSUSIYATLARI: AQSH TAJRIBASI MISOLIDA

Fathulla Xikmatov

Siyosiy fanlar bo'yicha falsafa doktori (PhD), dotsent
O'zbekiston Jurnalistika va ommaviy kommunikatsiyalar universiteti,
Siyosiy fanlar kafedrası

Abbos Jankayev

Xalqaro munosabatlar ta'lim yo'nalishi 4-kurs talabasi
abbosjankayev71@gmail.com
<https://doi.org/10.5281/zenodo.20389661>

ARTICLE INFO

Qabul qilindi: 22-may 2026 yil
Ma'qullandi: 24-may 2026 yil
Nashr qilindi: 26-may 2026 yil

KEYWORDS

Gibrid urush, AQSh, axborot urushi, kiberxavfsizlik, strategik raqobat, noan'anaviy tahdidlar, geosiyosat, irregulyar urush, propaganda, xalqaro xavfsizlik.

ABSTRACT

Mazkur maqolada gibrid urushlarning nazariy asoslari, tarixiy shakllanish jarayoni va zamonaviy xalqaro xavfsizlik tizimidagi o'rni AQSh tajribasi misolida ilmiy-tahliliy yondashuv asosida o'rganiladi. XXI asrda xalqaro munosabatlar tizimining murakkablashuvi, raqamli texnologiyalar rivoji va global geosiyosiy raqobatning kuchayishi natijasida urushlarning tabiati sezilarli darajada o'zgardi. Endilikda mojarolar faqat klassik jang maydonida emas, balki axborot, kiber, iqtisodiy va psixologik makonda ham olib borilmoqda. Shu sababli gibrid urush zamonaviy strategik xavfsizlik muhitining eng dolzarb fenomenlaridan biriga aylandi.

Maqolada Frank Hoffman, Ofer Fridman, Andrew Mumford, Liang va Xiangsui kabi olimlarning nazariy qarashlari asosida gibrid urush tushunchasining shakllanish omillari tahlil qilinadi. Shuningdek, gibrid urushning klassik urushdan farqli jihatlari, uning asosiy komponentlari va zamonaviy strategik xususiyatlari yoritiladi. Tadqiqot davomida AQShning Iroq va Afg'onistondagi operatsiyalari, terrorizmga qarshi global kampaniyalari, kiberxavfsizlik siyosati hamda 2016-yilgi prezidentlik saylovlariga tashqi aralashuv bilan bog'liq voqealar gibrid urushning amaliy ko'rinishlari sifatida tahlil qilinadi.

Tadqiqot natijalari shuni ko'rsatadiki, zamonaviy gibrid urushlarda harbiy vositalar yagona strategik instrument hisoblanmaydi. Axborot manipulyatsiyasi, kiberoperatsiyalar, iqtisodiy bosim, psixologik ta'sir va proksi tarmoqlar zamonaviy mojarolarning asosiy elementlariga aylangan. AQSh tajribasi esa zamonaviy mojaralarda konvensional ustunlik har doim ham strategik g'alabani kafolatlamasligini ko'rsatmoqda.

Maqola yakunida gibril tahdidlarga qarshi samarali kurash faqat harbiy emas, balki siyosiy, texnologik, informatsion va institutsional imkoniyatlarni birlashtirgan kompleks yondashuvni talab qilishi asoslanadi.

XXI asr boshlaridan boshlab xalqaro xavfsizlik tizimi tub transformatsiya jarayonini boshdan kechirmoqda. Globalizatsiya, raqamli texnologiyalar rivoji, transmilliy xavf-xatarlarning kuchayishi va geosiyosiy raqobatning murakkablashuvi natijasida zamonaviy mojarolarning tabiatida sezilarli o'zgarishlar yuz berdi. Endilikda urushlar faqat klassik jang maydonida emas, balki axborot makoni, iqtisodiy tizimlar, kiberfazo va jamoatchilik ongida ham olib borilmoqda. Shu sababli xalqaro munosabatlar va strategik tadqiqotlar tizimida "gibril urush" tushunchasi alohida ilmiy va siyosiy ahamiyat kasb etmoqda. Zamonaviy mojarolarning murakkablashuvi harbiy kuchning o'zi strategik ustunlikni ta'minlash uchun yetarli emasligini ko'rsatmoqda.

Sovuq urush tugaganidan keyin xalqaro tizimda an'anaviy davlatlararo harbiy mojarolar nisbatan kamaygan bo'lsa-da, bu global xavfsizlik muhiti barqarorlashganini anglatmadi. Aksincha, yangi davrda terrorizm, diniy-ekstremistik harakatlar, etnik mojarolar, kiberhujumlar va axborot manipulyatsiyasi kabi noan'anaviy tahdidlar kuchaydi. Ayniqsa, 2001-yil 11-sentabr voqealari zamonaviy xavfsizlik tizimi faqat klassik harbiy strategiyalar bilan himoyalaniishi mumkin emasligini yaqqol namoyon etdi. Ushbu voqealardan so'ng AQShning Afg'oniston va Iroqdagi operatsiyalari zamonaviy mojarolarda partizan usullari, terroristik tarmoqlar va media propogandasi strategik ahamiyat kasb etishini ko'rsatdi.

Gibril urush tushunchasi aynan mana shu murakkab xavfsizlik muhitini izohlash uchun shakllandi. Ushbu konsepsiya harbiy va noharbiy vositalarning yagona strategik maqsad yo'lida integratsiyalashgan holda qo'llanishini anglatadi. Zamonaviy gibril mojarolarda konvensional harbiy kuch bilan bir qatorda partizan taktikalari, kiberoperatsiyalar, iqtisodiy bosim, axborot manipulyatsiyasi va psixologik strategiyalar bir vaqtning o'zida qo'llanilishi mumkin. Shu jihatdan gibril urush an'anaviy urush modelidan sezilarli darajada farq qiladi.

Frank Hoffman gibril urushni XXI asr xavfsizlik muhitining eng muhim strategik fenomenlaridan biri sifatida tavsiflaydi. Uning fikricha, zamonaviy mojarolarning asosiy xususiyati turli urush shakllarining bir vaqtning o'zida qo'llanishida namoyon bo'ladi. Ofer Fridman esa gibril urush nazariyasining shakllanishini AQShning Iroq va Afg'onistondagi tajribasi bilan bog'laydi. Ushbu mojarolar AQShning yuqori texnologik va konvensional ustunligi strategik g'alabani avtomatik ravishda ta'minlamasligini ko'rsatdi. Bu esa zamonaviy xavfsizlik strategiyalarini qayta ko'rib chiqishga sabab bo'ldi.

Mavzuning dolzarbligi bir necha omillar bilan belgilanadi. Birinchidan, gibril tahdidlar zamonaviy xalqaro xavfsizlik tizimining eng murakkab va eng xavfli fenomenlaridan biriga aylandi. Ikkinchidan, gibril urush davlatlarning nafaqat harbiy salohiyatiga, balki siyosiy barqarorligi, iqtisodiy chidamliligi va informatsion xavfsizligiga ham bevosita ta'sir ko'rsatmoqda. Uchinchidan, sun'iy intellekt, ijtimoiy tarmoqlar va raqamli kommunikatsiyalar rivoji gibril operatsiyalarning ko'lamini yanada kengaytirmoqda. Ayniqsa, ijtimoiy media platformalarining siyosiy jarayonlarga ta'siri zamonaviy geosiyosiy raqobatda axborot omilining strategik ahamiyatini keskin oshirdi.

AQSh tajribasi gibril urush fenomenini o'rganishda alohida ilmiy ahamiyatga ega. Chunki mamlakat bir tomondan zamonaviy gibril tahdidlarning asosiy nishonlaridan biri bo'lsa, ikkinchi tomondan gibril strategiyalar va ularga qarshi kurash mexanizmlarini ishlab chiqayotgan global lider davlatlardan biridir. Iroq va Afg'onistondagi operatsiyalar, terrorizmga qarshi global kampaniyalar, 2016-yilgi prezidentlik saylovlariga tashqi aralashuv hamda kiberxavfsizlik bilan bog'liq voqealar gibril urushning zamonaviy ko'rinishlarini tahlil qilish uchun muhim empirik asos yaratadi.

Mazkur tadqiqotning asosiy maqsadi gibril urushlarning nazariy asoslari va zamonaviy xususiyatlarini AQSh tajribasi misolida ilmiy tahlil qilishdan iborat. Tadqiqot davomida gibril urush tushunchasining shakllanish omillari, uning klassik urushdan farqli jihatlari, axborot va kiber komponentlarining roli hamda zamonaviy geosiyosiy raqobatdagi o'rni tahlil qilinadi.

Tadqiqot metodologiyasi sifatida nazariy-komparativ tahlil, tarixiy yondashuv, kontent tahlil va keys-stadi metodlaridan foydalaniladi. Tadqiqotning manbaviy bazasini AQShning rasmiy strategik hujjatlari, xalqaro ilmiy jurnallar, xavfsizlik bo'yicha ekspertlarning ilmiy ishlari hamda zamonaviy geosiyosiy tahlillar tashkil etadi.

Maqolaning ilmiy yangiligi shundaki, unda gibril urush fenomeni AQSh tajribasi misolida faqat harbiy nuqtai nazardan emas, balki informatsion, kiber, iqtisodiy va psixologik komponentlarning o'zaro integratsiyasi asosida kompleks tarzda tahlil qilinadi. Bundan tashqari, maqolada zamonaviy raqamli texnologiyalar va sun'iy intellektning gibril urush strategiyalariga ta'siri ham alohida ko'rib chiqiladi.

Asosiy qism

1. Gibril urush tushunchasining nazariy asoslari va evolyutsiyasi

Gibril urush zamonaviy xalqaro xavfsizlik tizimining eng murakkab va ko'p qirrali fenomenlaridan biri sifatida shakllandi. XXI asr boshlaridan boshlab xalqaro mojarolarning xarakteri sezilarli darajada o'zgarib, an'anaviy urush modellarining chegaralari tobora xiralashib bormoqda. Endilikda davlatlar o'rtasidagi qarama-qarshilik faqat ochiq harbiy to'qnashuvlar orqali emas, balki axborot manipulyatsiyasi, kiberoperatsiyalar, iqtisodiy bosim, diplomatik ta'sir va psixologik strategiyalar orqali ham olib borilmoqda. Natijada zamonaviy urushning mazmuni va strategik tabiatini izohlash uchun yangi nazariy yondashuvlarga ehtiyoj paydo bo'ldi.

Gibril urush konsepsiyasining shakllanishi bir necha omillar bilan bog'liq. Birinchidan, Sovuq urushdan keyingi davrda global xavfsizlik muhiti tubdan o'zgardi. Ikki qutbli tizimning yemirilishi bilan klassik davlatlararo urushlar soni kamaygan bo'lsa-da, transmilliy terrorizm, diniy-ekstremistik harakatlar va asimmetrik tahdidlar kuchaya boshladi. Ikkinchidan, internet va raqamli texnologiyalar rivoji urushning operatsion makonini sezilarli darajada kengaytirdi. Axborot endilikda oddiy kommunikatsiya vositasi emas, balki strategik qurolga aylandi. Uchinchidan, AQShning yuqori texnologik harbiy ustunligi potensial raqiblarni to'g'ridan-to'g'ri harbiy qarama-qarshilikdan ko'ra aralash va asimmetrik strategiyalarni qo'llashga undadi.

Frank Hoffman gibril urush nazariyasini zamonaviy strategik tadqiqotlarda tizimlashtirgan eng muhim olimlardan biri hisoblanadi. Uning ta'kidlashicha, zamonaviy mojarolarning asosiy xususiyati turli urush shakllarining bir vaqtning o'zida qo'llanishida namoyon bo'ladi. Hoffman gibril urushni konvensional harbiy kuch, partizan taktikalari, terroristik usullar va kriminal faoliyatning yagona strategik maqsad yo'lida integratsiyalashgan holda qo'llanishi sifatida izohlaydi. Ushbu yondashuv zamonaviy xavfsizlik muhitining

murakkab tabiatini aks ettiradi. Chunki bugungi mojarolarda raqib har doim ham klassik armiya shaklida namoyon bo'lmaydi. Ko'pincha davlatlar nodavlat aktorlar, proksi tarmoqlar yoki anonim kiber guruhlar orqali ham strategik bosim o'tkazishi mumkin.

Ofer Fridman gibrud urush tushunchasining paydo bo'lishini AQShning Iroq va Afg'onistondagi tajribasi bilan bog'laydi. Uning fikricha, AQSh armiyasi jang maydonida mutlaq ustunlikka ega bo'lishiga qaramay, siyosiy va strategik barqarorlikni ta'minlashda murakkab muammolarga duch keldi. Partizan harakatlari, diniy-ekstremistik guruhlar va media propagandasi AQShning konvensional ustunligini sezilarli darajada murakkablashtirdi. Shu sababli zamonaviy mojarolarni faqat klassik urush nazariyalari orqali tushuntirish qiyinlashdi.

Gibrud urush nazariyasining shakllanishiga "to'rtinchi avlod urushi" konsepsiyasi ham katta ta'sir ko'rsatdi. Ushbu yondashuvga ko'ra, zamonaviy mojarolarda davlat monopoliyasi nisbatan zaiflashadi va nodavlat aktorlarning roli ortadi. Front va orqa hudud o'rtasidagi chegaralar yo'qoladi, jang esa ijtimoiy va psixologik makonga ko'chadi. Bu holat ayniqsa terroristik tarmoqlar va transmilliy ekstremistik harakatlar faoliyatida yaqqol namoyon bo'ldi. Zamonaviy mojarolarda axborot maydoni ham jang maydonining bir qismiga aylandi.

Liang va Xiangsui tomonidan ishlab chiqilgan "Cheklanmagan urush" konsepsiyasi ham gibrud urush nazariyasining rivojlanishida muhim o'rin tutadi. Mualliflarning ta'kidlashicha, zamonaviy raqobatda iqtisodiyot, texnologiya, diplomatiya va media ham harbiy qurol kabi strategik ahamiyat kasb etadi. Ular kelajakdagi mojarolar faqat jang maydonida emas, balki bank tizimi, internet, xalqaro savdo va kommunikatsiya platformalarida ham olib borilishini bashorat qilgan edi. Bugungi geosiyosiy raqobat aynan shu prognozning amaliy ifodasiga aylanmoqda.

Gibrud urushning tarixiy ildizlari yanada chuqurroq davrlarga borib taqaladi. Carl von Clausewitz urushni siyosatning boshqa vositalar bilan davom ettirilishi sifatida talqin qilgan. Zamonaviy gibrud urush ham aslida siyosiy maqsadga erishishga qaratilgan strategik faoliyat hisoblanadi. Biroq klassik modeldan farqli ravishda bu maqsadga faqat harbiy kuch orqali emas, balki iqtisodiy, axborot va psixologik bosim vositalari orqali ham erishiladi. Sun Tzu strategiyasida ham zamonaviy gibrud urush elementlari mavjud bo'lib, u axborot, aldov va psixologik ustunlikni harbiy muvaffaqiyatning muhim omili sifatida ko'radi.

Zamonaviy gibrud urushlarni tarixiy aralash urush shakllaridan ajratib turuvchi eng muhim omil texnologik komponent hisoblanadi. XX asrda propaganda asosan radio, gazeta va televideniye orqali olib borilgan bo'lsa, XXI asrda internet va ijtimoiy tarmoqlar millionlab auditoriyaga bir vaqtning o'zida ta'sir ko'rsatish imkoniyatini yaratdi. Algoritmik media tizimlari va sun'iy intellekt esa axborot manipulyatsiyasini yanada murakkablashtirdi. Deepfake texnologiyalari, avtomatlashtirilgan bot tarmoqlari va sun'iy intellekt yordamida yaratilgan propaganda zamonaviy informatsion mojarolarning yangi vositalariga aylandi.

Shuningdek, gibrud urushning muhim xususiyatlaridan biri uning noaniq xarakterga egaligidir. Klassik urushlarda hujum qiluvchi tomon odatda aniq bo'ladi. Gibrud urushda esa strategik bosim vositachi guruhlar, anonim kiberhujumlar yoki proksi tarmoqlar orqali amalga oshirilishi mumkin. Bu esa zamonaviy davlatlar uchun javob choralarini murakkablashtiradi va strategik noaniqlikni kuchaytiradi.

Bugungi xalqaro tizimda AQSh, Rossiya va Xitoy o'rtasidagi geosiyosiy raqobat tobora ko'proq gibrud xarakter kasb etmoqda. Ushbu davlatlar o'rtasidagi kurash faqat harbiy salohiyat bilan emas, balki texnologik ustunlik, axborot nazorati, iqtisodiy bosim va kiber

imkoniyatlar orqali ham olib borilmoqda. Shu sababli zamonaviy xalqaro xavfsizlik tizimida gibrud urush strategik raqobatning eng muhim shakllaridan biriga aylanmoqda.

Gibrud urushning klassik urushdan farqli jihatlari

Gibrud urush zamonaviy xalqaro xavfsizlik tizimida klassik urush modelidan tubdan farq qiluvchi strategik fenomen sifatida shakllandi. An'anaviy urushlarda asosiy rol muntazam armiyalar va ochiq harbiy to'qnashuvlarga tegishli bo'lgan bo'lsa, gibrud urushda harbiy va noharbiy vositalarning integratsiyalashgan holda qo'llanishi markaziy ahamiyat kasb etadi. Shu sababli zamonaviy mojarolarni tushunishda klassik va gibrud urush o'rtasidagi farqlarni tahlil qilish muhim ilmiy ahamiyatga ega.

Klassik urush modeli asosan Carl von Clausewitz strategik qarashlariga tayangan holda shakllangan. Ushbu yondashuvda urush davlatlar o'rtasidagi qurolli qarama-qarshilik sifatida talqin qilinadi va asosiy maqsad dushman armiyasini mag'lub etish hamda siyosiy iroda ustidan nazorat o'rnatishdan iborat bo'ladi. Zamonaviy gibrud urushda esa ushbu chegaralar sezilarli darajada xiralashadi. Endilikda qarama-qarshilik faqat jang maydonida emas, balki axborot makoni, iqtisodiyot, internet, diplomatik platformalar va psixologik muhitda ham olib boriladi. Bu esa zamonaviy mojarolarning operatsion hududini sezilarli darajada kengaytirdi.

Klassik urushlarda asosiy aktorlar davlat armiyalari hisoblangan bo'lsa, gibrud urushda nodavlat aktorlarning roli keskin ortdi. Terroristik tashkilotlar, diniy-ekstremistik harakatlar, xususiy harbiy kompaniyalar va transmilliy tarmoqlar zamonaviy mojarolarning faol ishtirokchisiga aylandi. Ayniqsa AQShning Iroq va Afg'onistondagi operatsiyalari ushbu tendensiyani yaqqol namoyon etdi. Ushbu mojaralarda asosiy qarshilik muntazam armiyalar tomonidan emas, balki partizan guruhlar, terroristik tarmoqlar va mahalliy qurolli harakatlar tomonidan amalga oshirildi. Natijada AQSh armiyasi yuqori texnologik ustunlikka ega bo'lishiga qaramay, uzoq muddatli strategik barqarorlikni ta'minlashda jiddiy muammolarga duch keldi.

Gibrud urushning muhim xususiyatlaridan biri uning ko'p domenli xarakteridir. Klassik urushlarda asosiy operatsion hudud quruqlik, dengiz va havo maydoni bilan cheklangan bo'lsa, zamonaviy gibrud mojaralarda kiberfazo va axborot muhiti ham to'laqonli jang maydoniga aylandi. Ayniqsa internet va ijtimoiy tarmoqlar rivoji axborotning strategik ahamiyatini keskin oshirdi. Endilikda davlatlar va nodavlat aktorlar millionlab insonlarning siyosiy qarashlariga masofadan turib ta'sir ko'rsatish imkoniyatiga ega bo'ldi. Shu jihatdan axborot manipulyatsiyasi zamonaviy gibrud urushning eng muhim elementlaridan biri hisoblanadi.

Klassik urushlarda propaganda ko'proq yordamchi vosita sifatida qo'llangan bo'lsa, gibrud urushda u strategik qurol darajasiga ko'tarildi. Dezinformatsiya, media manipulyatsiyasi, deepfake texnologiyalari va sun'iy intellekt yordamida yaratilgan kontent zamonaviy informatsion mojarolarning muhim vositalariga aylandi. Ayniqsa AQShdagi 2016-yilgi prezidentlik saylovlariga tashqi aralashuv bilan bog'liq voqealar axborot makonining geosiyosiy kurashdagi o'rnini yaqqol namoyon etdi. Ijtimoiy tarmoqlar orqali siyosiy polarizatsiyani kuchaytirish va jamoatchilik fikriga ta'sir ko'rsatish zamonaviy gibrud strategiyaning markaziy elementiga aylandi.

Gibrud urushning yana bir muhim jihati attribusiya muammosi bilan bog'liq. Klassik urushlarda hujum qiluvchi tomon odatda aniq bo'ladi. Gibrud urushda esa strategik bosim anonim kiberhujumlar, vositachi guruhlar yoki proksi tarmoqlar orqali amalga oshirilishi mumkin. Bu esa javob choralarni murakkablashtiradi va zamonaviy davlatlar uchun strategik

noaniqlikni kuchaytiradi. Ayniqsa kiberoperatsiyalar zamonaviy xavfsizlik tizimida eng murakkab tahdid shakllaridan biriga aylandi.

AQShga qarshi amalga oshirilgan SolarWinds va Colonial Pipeline kabi kiberhujumlar zamonaviy davlatlarning raqamli infratuzilmalari qanchalik zaif ekanligini ko'rsatdi. Ushbu hujumlar klassik harbiy bosqin shaklida bo'lmasa-da, davlat xavfsizligi va iqtisodiy tizimga jiddiy strategik ta'sir ko'rsatdi. Bu esa kiberfazoni zamonaviy urushning muhim operatsion maydoniga aylantirdi.

Gibrid urushning iqtisodiy komponenti ham zamonaviy mojarolarning ajralmas qismiga aylandi. Iqtisodiy sanksiyalar, texnologik embargolar va savdo urushlari geosiyosiy raqobatning strategik vositasi sifatida qo'llanilmoqda. Ayniqsa AQSh va Xitoy o'rtasidagi texnologik raqobat zamonaviy gibrid iqtisodiy qarama-qarshilikning yorqin misollaridan biri hisoblanadi. Yarimo'tkazgichlar, sun'iy intellekt va raqamli infratuzilma ustidan nazorat XXI asr strategik ustunligining muhim omiliga aylandi.

Shuningdek, gibrid urush psixologik bosim elementlari bilan ham ajralib turadi. Zamonaviy informatsion operatsiyalar aholida qo'rquv, siyosiy ishonchsizlik va ijtimoiy bo'linishni kuchaytirishga qaratiladi. Bu esa davlatning ichki barqarorligiga salbiy ta'sir ko'rsatadi hamda siyosiy qaror qabul qilish jarayonini murakkablashtiradi. Shu jihatdan zamonaviy gibrid urushning asosiy maqsadi ko'pincha dushmanni to'liq harbiy mag'lub etish emas, balki uning siyosiy va ijtimoiy tizimini zaiflashtirishdan iborat bo'ladi.

Jadval 1

Klassik va gibrid urushning qiyosiy tahlili

Mezoni	Klassik urush	Gibrid urush
Asosiy aktorlar	Davlat armiyalari	Davlat va nodavlat aktorlar
Operatsion makon	Jang maydoni	Ko'p domenli makon
Asosiy vosita	Harbiy kuch	Harbiy va noharbiy vositalar integratsiyasi
Axborot roli	Ikkinchi darajali	Strategik markaziy rol
Kiber komponent	Cheklangan	Asosiy elementlardan biri
Strategik maqsad	Harbiy g'alaba	Siyosiy va psixologik ustunlik
Urush shakli	Ochiq qarama-qarshilik	Noaniq va kombinatsiyalashgan

Shu tariqa, gibrid urush klassik urush modelidan nafaqat vositalari, balki strategik mantiqi bilan ham farqlanadi. Zamonaviy mojarolarda asosiy maqsad dushmanni faqat harbiy jihatdan mag'lub etish emas, balki uning siyosiy legitimligi, informatsion barqarorligi va ijtimoiy birligini zaiflashtirishdan iborat bo'lib bormoqda.

AQSh tajribasida gibrid urushning amaliy ko'rinishlari

XXI asrda AQSh gibrid urushning nafaqat nazariy, balki amaliy jihatdan ham eng muhim markazlaridan biriga aylandi. Mamlakat bir tomondan zamonaviy gibrid tahdidlarga qarshi kurash olib borayotgan global lider davlat sifatida namoyon bo'lsa, ikkinchi tomondan turli mojarolar davomida gibrid strategiyalardan faol foydalangan davlatlardan biri sifatida ham e'tirof etiladi. Ayniqsa Iroq va Afg'onistondagi harbiy operatsiyalar, terrorizmga qarshi global

kampaniyalar hamda kiberxavfsizlik bilan bog'liq voqealar AQSh tajribasida gibrud urushning amaliy shakllarini yaqqol namoyon etdi.

2001-yil 11-sentabr voqealaridan keyin AQSh "Global War on Terror" strategiyasini amalga oshirishni boshladi. Dastlab ushbu strategiya terroristik tashkilotlarni harbiy kuch yordamida yo'q qilishga qaratilgan edi. Biroq Afg'onistondagi operatsiyalar davomida AQSh armiyasi klassik jang maydonida ustunlikka erishgan bo'lsa-da, uzoq muddatli siyosiy barqarorlikni ta'minlashda murakkab muammolarga duch keldi. "Tolibon" harakati muntazam armiyaga ega bo'lmasa-da, partizan usullari, diniy propaganda va mahalliy aholi bilan ishlash orqali uzoq muddat davomida qarshilik ko'rsatishga muvaffaq bo'ldi. Bu esa zamonaviy mojarolarda harbiy ustunlik har doim ham strategik g'alabani ta'minlamasligini ko'rsatdi.

Iroqdagi vaziyat ham gibrud urushning murakkab tabiatini yaqqol namoyon etdi. 2003-yilda Saddam Husayn rejimi qisqa muddat ichida harbiy jihatdan mag'lub etilgan bo'lsa-da, keyingi davrda mamlakatda partizan harakatlari va diniy-ekstremistik guruhlar faoliyati keskin kuchaydi. Ayniqsa "Al-Qoida in Iraq" va keyinchalik "ISID"ning shakllanishi AQSh uchun yangi turdagi xavfsizlik tahdidini yuzaga keltirdi. Ushbu tashkilotlar harbiy operatsiyalar bilan bir qatorda media propagandasi, psixologik bosim va internet orqali radikallashuv strategiyalaridan ham faol foydalandi. Natijada urush klassik harbiy bosqichdan gibrud mojaroga aylandi.

AQSh tajribasida axborot komponentining ahamiyati ayniqsa muhim o'rin tutadi. Zamonaviy mojarolarda ommaviy axborot vositalari va ijtimoiy tarmoqlar strategik qurol darajasiga ko'tarildi. Terroristik tashkilotlar internet va media platformalar orqali nafaqat targ'ibot olib bordi, balki yangi a'zolari jalb qilish, psixologik bosim o'tkazish va jamoatchilik ongiga ta'sir ko'rsatishga ham muvaffaq bo'ldi. Ayniqsa ISID tomonidan ijtimoiy tarmoqlardan foydalanish usullari zamonaviy informatsion urushning yangi bosqichini boshlab berdi.

AQShdagi 2016-yilgi prezidentlik saylovlari bilan bog'liq voqealar ham gibrud urushning informatsion komponentini yaqqol namoyon etdi. Robert Mueller boshchiligidagi tergov natijalariga ko'ra, ijtimoiy tarmoqlar va raqamli platformalar orqali jamoatchilik fikriga ta'sir ko'rsatishga qaratilgan tashqi informatsion operatsiyalar amalga oshirilgan. Ushbu holat zamonaviy geosiyosiy qarama-qarshilikda axborotning strategik ahamiyatini keskin oshirdi. Endilikda saylov tizimlari, ijtimoiy media va jamoatchilik fikri ham milliy xavfsizlikning muhim elementi sifatida qaraladigan bo'ldi.

Kiberxavfsizlik masalasi ham AQSh tajribasida gibrud urushning markaziy yo'nalishlaridan biriga aylandi. XXI asrning ikkinchi o'n yilligidan boshlab AQSh davlat tizimlari va muhim infratuzilmalariga qarshi yirik kiberhujumlar soni sezilarli darajada ortdi. Ayniqsa SolarWinds va Colonial Pipeline bilan bog'liq hodisalar davlatning energetika, kommunikatsiya va boshqaruv tizimlari raqamli tahdidlarga qanchalik zaif ekanligini ko'rsatdi. Ushbu hujumlar to'g'ridan-to'g'ri harbiy bosqin bo'lmasa-da, iqtisodiy xavfsizlik va milliy barqarorlikka jiddiy strategik ta'sir ko'rsatdi.

AQSh bunga javoban kiberxavfsizlik strategiyasini kuchaytirishga kirishdi. 2009-yilda U.S. Cyber Command tashkil etilishi zamonaviy raqamli tahdidlarga qarshi kurashni yangi bosqichga olib chiqdi. Pentagonning keyingi strategik hujjatlarida kiberfazo quruqlik, dengiz va havo maydoni bilan teng darajadagi operatsion hudud sifatida e'tirof etildi. Bu esa zamonaviy urushning ko'p domenli xarakterga ega ekanligini ko'rsatadi.

AQSh va Xitoy o'rtasidagi texnologik raqobat ham zamonaviy gibril qarama-qarshilikning muhim ko'inishiga aylandi. Yarimo'tkazgichlar, sun'iy intellekt, 5G texnologiyalari va raqamli infratuzilma ustidan nazorat XXI asr strategik raqobatining asosiy yo'nalishlaridan biri hisoblanmoqda. Texnologik embargolar va iqtisodiy cheklovlar endilikda harbiy vositalar kabi geosiyosiy bosim instrumentiga aylanmoqda. Shu sababli zamonaviy gibril urushda iqtisodiy va texnologik ustunlik strategik xavfsizlikning asosiy omillaridan biri sifatida qaralmoqda.

AQShning gibril tahdidlarga qarshi strategiyasi va zamonaviy xavfsizlik siyosati

Zamonaviy xalqaro xavfsizlik muhiti AQShni gibril tahdidlarga qarshi yangi strategik yondashuvlarni ishlab chiqishga majbur qildi. XXI asr boshlarida terrorizmga qarshi kurash asosiy xavfsizlik yo'nalishi sifatida qaralgan bo'lsa, keyingi davrda kiberxavfsizlik, axborot manipulyatsiyasi, iqtisodiy bosim va texnologik raqobat ham milliy xavfsizlikning markaziy elementlariga aylandi. Natijada AQSh strategik siyosati klassik harbiy mudofaa modelidan ko'p domenli va kompleks xavfsizlik tizimiga o'ta boshladi.

AQSh Mudofaa vazirligi tomonidan ishlab chiqilgan yangi strategik hujjatlarda gibril tahdidlar milliy xavfsizlikka qarshi eng murakkab xavf shakllaridan biri sifatida qayd etiladi. Pentagonning 2018 va 2022-yillardagi milliy mudofaa strategiyalarida Rossiya va Xitoy asosiy geosiyosiy raqib sifatida ko'rsatilgan bo'lib, ushbu davlatlar bilan qarama-qarshilik faqat harbiy emas, balki iqtisodiy, texnologik, axborot va kiber makonda ham davom etayotgani ta'kidlanadi. Bu esa zamonaviy strategik raqobatning gibril xarakter kasb etganini anglatadi.

AQShning gibril tahdidlarga qarshi strategiyasida kiberxavfsizlik alohida o'rin egallaydi. Zamonaviy davlat boshqaruvi, energetika tizimi, moliya sektori va kommunikatsiya infratuzilmalari raqamli texnologiyalarga bog'liq bo'lib qolgani sababli kiberhujumlar milliy xavfsizlikka jiddiy tahdid sifatida qaralmoqda. Ayniqsa SolarWinds hodisasi AQSh davlat tizimlari va federal agentliklarining kiber himoya mexanizmlarida jiddiy zaifliklar mavjudligini ko'rsatdi. Ushbu voqeadan so'ng AQSh hukumati davlat va xususiy sektor o'rtasidagi kiberhamkorlikni kuchaytirishga kirishdi.

Kiberxavfsizlik strategiyasining muhim elementlaridan biri "Cyber Command" faoliyati bilan bog'liq. Ushbu tuzilma nafaqat mudofaa, balki preventiv va javob xarakteridagi kiberoperatsiyalarni ham amalga oshirish vakolatiga ega bo'ldi. Natijada AQSh kiberfazoni quruqlik, dengiz va havo maydoni bilan teng darajadagi strategik operatsion hudud sifatida qabul qila boshladi. Bu esa zamonaviy urushning ko'p domenli tabiatini aks ettiradi.

AQSh strategiyasida axborot xavfsizligi masalasi ham markaziy o'rin tutadi. 2016-yilgi prezidentlik saylovlariga tashqi aralashuv bilan bog'liq voqealar AQSh siyosiy tizimining informatsion tahdidlarga nisbatan zaifligini ochib berdi. Ayniqsa ijtimoiy tarmoqlar orqali dezinformatsiya kampaniyalari olib borilishi jamoatchilik fikrini boshqarish zamonaviy geosiyosiy kurashning muhim vositasiga aylanganini ko'rsatdi. Shu sababli AQSh hukumati ijtimoiy media platformalari ustidan nazoratni kuchaytirish, feyk axborotlarni aniqlash va raqamli savodxonlikni oshirish bo'yicha yangi dasturlar ishlab chiqdi.

Sun'iy intellekt texnologiyalarining rivojlanishi ham AQSh xavfsizlik strategiyasiga sezilarli ta'sir ko'rsatmoqda. Pentagon va DARPA tomonidan ishlab chiqilayotgan sun'iy intellekt tizimlari zamonaviy harbiy va razvedka operatsiyalarida muhim rol o'ynamoqda. Shu bilan birga AI texnologiyalari deepfake, avtomatlashtirilgan propaganda va raqamli manipulyatsiya kabi yangi tahdidlarni ham yuzaga keltirmoqda. Natijada AQSh strategik hujjatlarida sun'iy intellekt ham imkoniyat, ham xavf manbai sifatida talqin qilinmoqda.

AQShning gibridda tahdidlarga qarshi siyosatida iqtisodiy xavfsizlik ham alohida ahamiyat kasb etadi. Ayniqsa AQSh va Xitoy o'rtasidagi texnologik raqobat zamonaviy iqtisodiy gibridda qarama-qarshilikning markaziy yo'nalishiga aylandi. Yarimo'tkazgichlar ishlab chiqarishi, sun'iy intellekt va 5G texnologiyalari ustidan nazorat XXI asr geosiyosiy ustunligining asosiy omillaridan biri sifatida qaralmoqda. AQSh tomonidan Huawei va boshqa texnologik kompaniyalarga qarshi joriy etilgan cheklovlar zamonaviy iqtisodiy bosim vositalarining amaliy ko'rinishi hisoblanadi.

Bundan tashqari, AQShning zamonaviy xavfsizlik strategiyasi "whole-of-government approach" tamoyiliga asoslanmoqda. Ushbu yondashuvga ko'ra, gibridda tahdidlarga qarshi kurash faqat harbiy institutlarning vazifasi emas. Davlat boshqaruvi organlari, razvedka xizmatlari, texnologik kompaniyalar, diplomatik institutlar va fuqarolik jamiyati o'rtasidagi hamkorlik milliy xavfsizlikning muhim elementi sifatida qaralmoqda. Bu esa zamonaviy gibridda mojarolarning kompleks xarakterini aks ettiradi.

Iroq va Afg'oniston urushlarida gibridda qarshilik modeli

AQSh tajribasida Iroq va Afg'oniston urushlari gibridda urushning amaliy ko'rinishlarini tushunish uchun eng muhim empirik maydonlardan biri hisoblanadi. Har ikki holatda ham AQSh dastlab an'anaviy harbiy ustunlik orqali tezkor muvaffaqiyatga erishdi, biroq keyingi bosqichlarda mojaro klassik urush shaklidan chiqib, partizan taktikasi, terroristik harakatlar, axborot propagandasi, mahalliy ijtimoiy tarmoqlar va siyosiy legitimlik uchun kurash bilan bog'liq gibridda xarakter kasb etdi. Bu esa zamonaviy urushlarda harbiy g'alaba strategik barqarorlikni avtomatik ravishda ta'minlamasligini ko'rsatdi.

2003-yilda Iroqda Saddam Husayn rejimi qisqa vaqt ichida harbiy jihatdan mag'lub etildi. AQSh va koalitsion kuchlar konvensional jang maydonida mutlaq ustunlikka ega edi. Biroq rejim ag'darilganidan keyingi davrda xavfsizlik vakuumi yuzaga keldi va bu holat turli mahalliy hamda transmilliy qurolli guruhlarning faollashuviga sharoit yaratdi. Sobiq Baas partiyasi tarafdorlari, sunniy qo'zg'olonchi guruhlar, "Al-Qoida in Iraq" va keyinchalik "Islomiy davlat" kabi tuzilmalar Iroqdagi mojaroni an'anaviy urush bosqichidan gibridda qarshilik bosqichiga olib chiqdi. Ushbu guruhlar AQSh armiyasi bilan ochiq jang qilishdan ko'ra portlovchi qurilmalar, pistirma, shahar muhitidagi janglar, propaganda va qo'rquv strategiyasiga tayandilar.

Iroqdagi gibridda qarshilikning eng muhim xususiyatlaridan biri uning arzon, moslashuvchan va psixologik jihatdan kuchli ta'sir ko'rsatadigan vositalarga tayanishi edi. Ayniqsa qo'lbola portlovchi qurilmalar AQSh harbiy texnikasi va patrul tizimlariga katta zarar yetkazdi. Bu vositalar yuqori texnologik harbiy kuchga ega davlatga qarshi past xarajatli, ammo yuqori siyosiy va psixologik ta'sirga ega usul sifatida qo'llanildi. Shu bilan birga, qo'zg'olonchi guruhlar harbiy hujumlarni media materiallar bilan birlashtirib, AQSh yo'qotishlarini ommaviy axborot maydonida kuchaytirishga intildilar. Natijada jang maydonidagi kichik operatsiyalar global axborot maydonida katta strategik ta'sirga ega bo'ldi.

Afg'oniston urushi ham gibridda qarshilikning boshqa bir murakkab shaklini namoyon etdi. 2001-yilda AQSh boshchiligidagi operatsiyalar Tolibon hukumatini qisqa muddatda ag'darishga muvaffaq bo'ldi. Biroq Tolibon to'liq yo'qolmadi, balki mahalliy ijtimoiy tuzilmalar, diniy legitimlik, qabila aloqalari va geografik murakkablikdan foydalangan holda uzoq muddatli qarshilik strategiyasiga o'tdi. Ular AQSh va NATO kuchlariga qarshi ochiq konvensional jang olib borishdan qochib, vaqtini strategik qurol sifatida ishlatdi. Mojaroning cho'zilishi AQSh

jamiyatida siyosiy charchoqni kuchaytirdi va urushni davom ettirishga bo'lgan ichki siyosiy qo'llab-quvvatlovni pasaytirdi.

Afg'onistondagi gibridd qarshilik Iroqdan farqli ravishda geografik va ijtimoiy omillar bilan yanada chambarchas bog'liq edi. Tog'li hududlar, markaziy hukumat nazoratining cheklanganligi, chegaradosh hududlardagi boshpana imkoniyatlari va mahalliy qabila tizimi Tolibonga uzoq muddatli omon qolish imkonini berdi. Shu bilan birga, Tolibon o'z harakatlarini diniy va milliy ozodlik narrativi bilan asoslab, AQSh va NATO kuchlarini "xorijiy bosqinchi" sifatida tasvirlashga harakat qildi. Bu esa axborot va psixologik urushning mahalliy darajadagi samaradorligini oshirdi.

Iroq va Afg'oniston tajribasi AQSh strategik tafakkurida muhim o'zgarishlarga sabab bo'ldi. Dastlab harbiy kuch orqali tezkor g'alabaga erishish mumkin degan tasavvur ustun bo'lgan bo'lsa, keyinchalik siyosiy legitimlik, mahalliy boshqaruv, aholi ishonchi, axborot ustunligi va iqtisodiy tiklanish kabi omillar urush natijasini belgilovchi asosiy elementlar sifatida qarala boshlandi. Shu sababli AQSh harbiy doktrinasida counterinsurgency yondashuvi kuchaydi. Ushbu yondashuvda asosiy e'tibor dushmanni faqat jismonan yo'q qilishga emas, balki aholi bilan munosabatni yaxshilash, mahalliy institutlarni mustahkamlash va siyosiy legitimlikni tiklashga qaratildi.

Iroq va Afg'oniston urushlari gibridd urushning eng asosiy sabog'ini namoyon etdi: zamonaviy mojarolarda konvensional harbiy g'alaba siyosiy g'alabaga teng emas. AQSh jang maydonida yirik harbiy muvaffaqiyatlarga erishgan bo'lsa-da, uzoq muddatli barqarorlikni ta'minlashda katta qiyinchiliklarga duch keldi. Bu esa gibridd urushda strategik natija ko'pincha harbiy kuchdan ko'ra siyosiy legitimlik, axborot nazorati va mahalliy muhitni tushunish qobiliyati bilan belgilanadi, degan xulosani tasdiqlaydi.

Axborot urushi va media manipulyatsiyasining gibridd mojarolardagi o'rni

Zamonaviy gibridd urushlarda axborot omili strategik ahamiyat kasb etuvchi eng muhim komponentlardan biriga aylandi. XXI asrda internet, ijtimoiy tarmoqlar va raqamli kommunikatsiyalar rivoji natijasida informatsion makon urushning alohida operatsion hududiga aylandi. Endilikda davlatlar va nodavlat aktorlar jamoatchilik fikriga ta'sir ko'rsatish, siyosiy qarorlarni shakllantirish hamda ijtimoiy beqarorlikni kuchaytirish uchun axborot vositalaridan faol foydalanmoqda. Shu sababli zamonaviy mojarolarda informatsion ustunlik ko'pincha harbiy ustunlikdan kam bo'lmagan strategik ahamiyatga ega bo'lib qolmoqda.

Axborot urushi klassik propaganda modelidan sezilarli darajada farq qiladi. XX asrda propaganda asosan davlat nazoratidagi televideniye, radio va matbuot orqali amalga oshirilgan bo'lsa, XXI asrda ijtimoiy tarmoqlar axborot tarqatishning asosiy platformasiga aylandi. Facebook, X (Twitter), YouTube va Telegram kabi platformalar millionlab auditoriyaga qisqa vaqt ichida ta'sir ko'rsatish imkoniyatini yaratdi. Natijada axborot manipulyatsiyasi markazlashgan davlat propagandasidan decentralizatsiyalashgan va algoritmik boshqariladigan tizimga o'tdi.

AQSh tajribasi zamonaviy axborot urushining murakkab xarakterini yaqqol namoyon etdi. Ayniqsa 2016-yilgi prezidentlik saylovlari bilan bog'liq voqealar ijtimoiy tarmoqlarning geosiyosiy raqobatdagi rolini keskin oshirdi. Robert Mueller boshchiligidagi tergov hisobotida ijtimoiy media platformalari orqali jamoatchilik fikriga ta'sir ko'rsatishga qaratilgan tashqi informatsion operatsiyalar amalga oshirilgani qayd etildi. Ushbu kampaniyalarda soxta akkauntlar, bot tarmoqlari va manipulyativ media kontentdan foydalanilgan. Maqsad AQSh

jamiyatida siyosiy polarizatsiyani kuchaytirish va jamoatchilik ishonchini zaiflashtirishdan iborat edi.

Axborot urushining muhim xususiyatlaridan biri shundaki, unda asosiy maqsad ko'pincha dushmani to'g'ridan-to'g'ri mag'lub etish emas, balki jamiyat ichida ishonchsizlik va bo'linishni kuchaytirish hisoblanadi. Zamonaviy informatsion operatsiyalar aholini qo'rqitish, siyosiy institutlarga bo'lgan ishonchni kamaytirish va ijtimoiy konfliktlarni chuqurlashtirishga qaratiladi. Shu sababli axborot urushi gibril strategiyaning psixologik komponenti bilan chambarchas bog'liq.

Iroq va Afg'oniston mojarolari davomida terroristik tashkilotlar ham media va internet imkoniyatlaridan faol foydalandilar. Ayniqsa ISID tomonidan ijtimoiy tarmoqlarda olib borilgan propaganda kampaniyalari zamonaviy informatsion urushning yangi bosqichini boshlab berdi. Ushbu tashkilot professional media mahsulotlari, videolar va internet targ'iboti orqali nafaqat Yaqin Sharq, balki Yevropa va AQShdagi auditoriyaga ham ta'sir ko'rsatishga muvaffaq bo'ldi. Shu tariqa internet terroristik tashkilotlar uchun global kommunikatsion platformaga aylandi.

Sun'iy intellekt texnologiyalarining rivojlanishi axborot urushini yanada murakkablashtirdi. Deepfake texnologiyalari yordamida yaratilgan videolar, AI-generated kontent va avtomatlashtirilgan bot tarmoqlari informatsion manipulyatsiyaning yangi shakllarini yuzaga keltirmoqda. Endilikda soxta axborotni haqiqiy ma'lumotdan ajratish tobora qiyinlashmoqda. Bu esa zamonaviy davlatlar uchun nafaqat texnologik, balki siyosiy va ijtimoiy xavfsizlik muammosini ham yuzaga keltirmoqda.

AQSh hukumati ushbu tahdidlarga qarshi kurashish maqsadida bir qator strategik choralarini amalga oshirmoqda. Xususan, kiberxavfsizlik va axborot xavfsizligi bo'yicha federal dasturlar kengaytirildi, ijtimoiy media platformalari bilan hamkorlik kuchaytirildi hamda dezinformatsiyaga qarshi maxsus monitoring tizimlari yaratildi. Bundan tashqari, raqamli savodxonlikni oshirish va feyk axborotlarni aniqlash bo'yicha ta'lim dasturlariga ham alohida e'tibor qaratilmoqda.

Shu bilan birga, axborot urushiga qarshi kurash demokratik jamiyatlarda murakkab muammo hisoblanadi. Chunki bir tomondan davlat milliy xavfsizlikni ta'minlash uchun dezinformatsiyaga qarshi choralar ko'rishga intiladi, ikkinchi tomondan esa so'z erkinligi va demokratik qadriyatlarni saqlab qolish zarurati mavjud. AQSh tajribasi shuni ko'rsatadiki, zamonaviy informatsion tahdidlarga qarshi samarali kurash texnologik himoya bilan bir qatorda jamiyatning media savodxonligi va institutsional barqarorligiga ham bog'liq.

Zamonaviy gibril mojaralarda axborot ustidan nazorat strategik ustunlikning muhim omiliga aylandi. Shu sababli XXI asr xavfsizlik muhitida media, internet va kommunikatsion texnologiyalar harbiy strategiya bilan teng darajadagi geosiyosiy instrument sifatida qaralmoqda. Bu esa axborot urushini zamonaviy gibril qarama-qarshilikning eng muhim yo'nalishlaridan biriga aylantirmoqda.

Kiberurush va raqamli texnologiyalarning gibril mojarolardagi roli

XXI asrda raqamli texnologiyalar rivojlanishi xalqaro xavfsizlik tizimining xarakterini tubdan o'zgartirdi. Internet, sun'iy intellekt, bulutli texnologiyalar va global kommunikatsion tarmoqlarning kengayishi natijasida kiberfazo zamonaviy mojarolarning muhim operatsion maydoniga aylandi. Shu sababli gibril urushning eng muhim komponentlaridan biri sifatida kiberurush tushunchasi shakllandi. Endilikda davlatlar va nodavlat aktorlar strategik

maqsadlarga erishish uchun raqamli infratuzilmalar, davlat boshqaruvi tizimlari va kommunikatsion tarmoqlarga qarshi kiberoperatsiyalardan faol foydalanmoqda.

Kiberurush klassik harbiy hujumlardan bir qator jihatlari bilan farq qiladi. Birinchidan, kiberoperatsiyalar geografik chegaralarni deyarli tan olmaydi. Zamonaviy davlatning energetika, bank-moliya, transport va kommunikatsiya tizimlari internet orqali global tarmoqqa bog'langanligi sababli har qanday davlat masofadan turib hujum obyektiga aylanishi mumkin. Ikkinchidan, kiberhujumlarni amalga oshirayotgan subyektning aniqlash murakkab bo'ladi. Ko'pincha hujumlar anonim guruhlar, vositachi tarmoqlar yoki proksi serverlar orqali amalga oshiriladi. Bu esa javob choralarni murakkablashtiradi va strategik noaniqlikni kuchaytiradi.

AQSh zamonaviy kiber tahdidlarga eng ko'p duch kelayotgan davlatlardan biri hisoblanadi. Mamlakatning iqtisodiy va harbiy salohiyati yuqori darajada raqamli infratuzilmaga bog'langanligi sababli kiberxavfsizlik milliy xavfsizlikning markaziy yo'nalishiga aylandi. Ayniqsa so'nggi o'n yillikda AQSh davlat institutlari, xususiy kompaniyalari va strategik infratuzilmalariga qarshi yirik kiberhujumlar soni sezilarli darajada ortdi. Bu holat kiberfazoni zamonaviy geosiyosiy raqobatning eng faol maydonlaridan biriga aylantirdi.

2020-yildagi SolarWinds hodisasi AQSh tarixidagi eng yirik kiberjosuslik operatsiyalaridan biri sifatida baholanadi. Ushbu hujum davomida federal agentliklar va yirik kompaniyalarning dasturiy ta'minot tizimlariga zararli kod joylashtirilgan. Natijada minglab tashkilotlarning ma'lumotlari xavf ostida qoldi. Ushbu hodisa AQShning strategik infratuzilmasi qanchalik raqamli xavflarga bog'liq ekanligini namoyon etdi. Shu bilan birga, kiberhujumlarning iqtisodiy va siyosiy oqibatlari klassik harbiy hujumlar bilan taqqoslanadigan darajada bo'lishi mumkinligi ma'lum bo'ldi.

Colonial Pipeline bilan bog'liq hodisa esa kiberurushning iqtisodiy xavfsizlikka ta'sirini yaqqol ko'rsatdi. 2021-yilda amalga oshirilgan kiberhujum AQShdagi eng yirik yonilg'i quvur tizimlaridan birining vaqtincha faoliyatini to'xtatdi. Natijada bir qator shtatlarda yonilg'i taqchilligi va iqtisodiy beqarorlik yuzaga keldi. Ushbu voqea kiberhujumlar zamonaviy davlatning kundalik iqtisodiy hayotiga ham jiddiy ta'sir ko'rsatishi mumkinligini ko'rsatdi.

AQSh ushbu tahdidlarga javoban kiberxavfsizlik strategiyasini kuchaytirdi. 2009-yilda tashkil etilgan U.S. Cyber Command zamonaviy kiberoperatsiyalarni muvofiqlashtiruvchi asosiy harbiy tuzilmaga aylandi. Pentagonning strategik hujjatlarida kiberfazo quruqlik, dengiz va havo maydoni bilan teng darajadagi operatsion domen sifatida tan olindi. Bu esa zamonaviy urushning ko'p domenli xarakterini yana bir bor tasdiqlaydi.

Kiberurushning muhim jihatlardan biri uning gibridd strategiyalar bilan integratsiyalashgan holda qo'llanishidir. Zamonaviy mojaralarda kiberoperatsiyalar ko'pincha axborot manipulyatsiyasi, iqtisodiy bosim va diplomatik strategiyalar bilan birga olib boriladi. Masalan, saylov tizimlariga kiberaralashuv, ijtimoiy tarmoqlarda dezinformatsiya kampaniyalari va iqtisodiy ma'lumotlarni o'g'irlash operatsiyalari yagona strategik maqsad doirasida amalga oshirilishi mumkin. Shu sababli kiberurush gibridd urushning markaziy komponentlaridan biriga aylandi.

Sun'iy intellekt texnologiyalarining rivojlanishi kiberxavfsizlik muhitini yanada murakkablashtirmoqda. AI yordamida avtomatlashtirilgan kiberhujumlar, zararli dasturlarni tezkor moslashtirish va ma'lumotlarni tahlil qilish imkoniyatlari ortmoqda. Shu bilan birga,

sun'iy intellekt himoya tizimlarini ham kuchaytirish imkonini bermoqda. Natijada zamonaviy kiberfazoda hujum va himoya o'rtasidagi raqobat yangi bosqichga ko'tarildi.

AQSh va Xitoy o'rtasidagi texnologik raqobat ham kiberurushning geosiyosiy ahamiyatini oshirmoqda. Sun'iy intellekt, yarimo'tkazgichlar, kvant texnologiyalari va 5G tizimlari ustidan nazorat XXI asr strategik ustunligining asosiy omillaridan biri sifatida qaralmoqda. Shu sababli texnologik salohiyat zamonaviy davlatning harbiy qudrati bilan teng darajadagi xavfsizlik komponentiga aylandi.

Zamonaviy geosiyosiy raqobatda gibril urushning o'rni

Zamonaviy xalqaro munosabatlarda gibril urush faqat harbiy taktika yoki xavfsizlik texnologiyasi emas, balki yirik davlatlar o'rtasidagi strategik raqobatning asosiy shakllaridan biriga aylanmoqda. AQSh, Rossiya va Xitoy o'rtasidagi geosiyosiy qarama-qarshilik tobora ko'proq ochiq harbiy to'qnashuvdan ko'ra axborot, iqtisodiyot, texnologiya, kiberfazo va diplomatik bosim maydonlarida namoyon bo'lmoqda. Bu holat zamonaviy xalqaro tizimda "kulrang zona" deb ataluvchi oraliq holatlarning kengayishiga olib keldi. Bunday vaziyatda davlatlar rasmiy urush e'lon qilmasdan turib, raqibining siyosiy irodasi, iqtisodiy barqarorligi va xalqaro mavqeiga ta'sir ko'rsatishga intiladi.

AQSh strategik hujjatlarida so'nggi yillarda Rossiya va Xitoy bilan raqobat milliy xavfsizlikning asosiy yo'nalishi sifatida belgilanmoqda. Rossiya bilan qarama-qarshilik ko'proq axborot operatsiyalari, kiberhujumlar, energetika siyosati, proksi kuchlardan foydalanish va NATOning sharqiy qanotidagi xavfsizlik muammolari orqali namoyon bo'lmoqda. Xitoy bilan raqobat esa asosan texnologik ustunlik, savdo tizimi, sun'iy intellekt, yarimo'tkazgichlar va Indo-Tinch okeani mintaqasidagi harbiy-siyosiy muvozanat atrofida shakllanmoqda. Shu jihatdan gibril urush zamonaviy strategik raqobatda harbiy kuch bilan iqtisodiy va texnologik vositalar o'rtasidagi chegarani xiralashtirmoqda.

Rossiya tajribasi gibril urush tushunchasining xalqaro siyosatda keng muhokama qilinishiga kuchli ta'sir ko'rsatdi. Ayniqsa 2014-yildagi Qrim voqealari G'arb strategik doiralarida gibril urush fenomeniga bo'lgan e'tiborni keskin oshirdi. Ushbu jarayonda harbiy kuch, siyosiy bosim, mahalliy proksi tuzilmalar, axborot kompaniyalari va huquqiy manipulyatsiya elementlari birgalikda qo'llanilgani qayd etildi. Bu holat zamonaviy mojaralarda rasmiy urush va tinchlik o'rtasidagi chegaraning tobora noaniqlashib borayotganini ko'rsatdi. Biroq ayrim tadqiqotchilar "Gerasimov doktrinasi" atamasi ilmiy va siyosiy diskursda ba'zan ortiqcha soddalashtirilgan holda ishlatilishini ham ta'kidlaydilar.

Xitoy bilan bog'liq gibril raqobat esa asosan iqtisodiy va texnologik maydonda namoyon bo'lmoqda. Xitoyning "Bir makon — bir yo'l" tashabbusi, global infratuzilma investitsiyalari, raqamli texnologiyalar eksporti va 5G tarmoqlaridagi faoliyati AQSh tomonidan nafaqat iqtisodiy, balki strategik xavfsizlik masalasi sifatida talqin qilinmoqda. Bu raqobatda harbiy bosim ikkinchi darajali ko'rinishda bo'lsa-da, texnologik bog'liqlik, raqamli standartlar va ma'lumotlar xavfsizligi asosiy geosiyosiy omilga aylanmoqda. Shu sababli XXI asr gibril urushi faqat frontdagi janglar emas, balki global texnologik ekotizimlar ustidan nazorat uchun kurash sifatida ham namoyon bo'lmoqda.

NATO doirasida ham gibril tahdidlarga qarshi kurash muhim strategik yo'nalishga aylandi. Alyans hujjatlarida gibril tahdidlar harbiy, kiber, iqtisodiy va informatsion bosimlarning uyg'unlashgan shakli sifatida talqin qilinadi. NATO uchun bunday tahdidlarning murakkabligi shundaki, ular ko'pincha 5-modda doirasida klassik harbiy hujum sifatida

baholash qiyin bo'lgan shaklda amalga oshiriladi. Masalan, kiberhujum, dezinformatsiya kampaniyasi yoki energetika bosimi davlat xavfsizligiga jiddiy zarar yetkazishi mumkin, biroq unga javob berish mexanizmi klassik harbiy hujumga nisbatan ancha murakkab bo'ladi.

Zamonaviy geosiyosiy raqobatda gibrud urushning ahamiyati shundaki, u davlatlarga ochiq urush xavfini oshirmasdan raqibga bosim o'tkazish imkonini beradi. Bu strategiya ayniqsa yirik davlatlar o'rtasida to'g'ridan-to'g'ri harbiy to'qnashuv xavfi yuqori bo'lgan sharoitda qo'llaniladi. Chunki yadroviy qurolga ega davlatlar o'rtasida ochiq urush global falokatga olib kelishi mumkin. Shu bois siyosiy ta'sir, kiberoperatsiyalar, sanksiyalar, texnologik cheklovlar va axborot kampaniyalari zamonaviy strategik raqobatning nisbatan "nazorat qilinadigan" vositalariga aylanmoqda.

AQSh tajribasi shuni ko'rsatadiki, gibrud urushga qarshi samarali javob faqat mudofaa tizimini kuchaytirish bilan cheklanmaydi. Davlat axborot makoni, iqtisodiy tizim, texnologik infratuzilma, saylov xavfsizligi va xalqaro ittifoqlarni yagona strategik tizim sifatida ko'rishi kerak. Aynan shu sababli AQSh so'nggi yillarda NATO, Yevropa Ittifoqi va Indo-Tinch okeani mintaqasidagi hamkorlari bilan gibrud tahdidlarga qarshi koordinatsiyani kuchaytirmoqda. Bu jarayon zamonaviy xavfsizlik siyosatida kollektiv javob mexanizmlarining ahamiyati oshib borayotganini ko'rsatadi.

Xulosa

XXI asr xalqaro xavfsizlik tizimida gibrud urush eng murakkab va ko'p qirrali strategik fenomenlardan biriga aylandi. Globalizatsiya, raqamli texnologiyalar rivoji va geosiyosiy raqobatning kuchayishi natijasida zamonaviy mojarolar klassik urush modelidan sezilarli darajada farq qila boshladi. Endilikda davlatlar o'rtasidagi qarama-qarshilik faqat ochiq harbiy to'qnashuvlar orqali emas, balki axborot manipulyatsiyasi, kiberoperatsiyalar, iqtisodiy bosim, psixologik strategiyalar va texnologik raqobat orqali ham olib borilmoqda. Shu sababli gibrud urush zamonaviy xalqaro munosabatlar tizimining ajralmas qismiga aylandi.

Tadqiqot davomida gibrud urush tushunchasining nazariy asoslari tahlil qilindi va uning klassik urushdan farqli jihatlari yoritildi. Frank Hoffman, Ofer Fridman, Lawrence Freedman va boshqa tadqiqotchilarning ilmiy qarashlari shuni ko'rsatadiki, zamonaviy gibrud mojarolarning asosiy xususiyati harbiy va noharbiy vositalarning yagona strategik maqsad yo'lida integratsiyalashgan holda qo'llanishidir. Bu esa gibrud urushni oddiy harbiy qarama-qarshilik emas, balki kompleks siyosiy va strategik jarayon sifatida talqin qilish zarurligini ko'rsatadi.

AQSh tajribasi gibrud urushning amaliy mohiyatini tushunishda muhim empirik asos bo'lib xizmat qiladi. Iroq va Afg'oniston urushlari zamonaviy mojarolarda konvensional harbiy ustunlik strategik g'alabani avtomatik ravishda ta'minlamasligini namoyon etdi. Partizan taktikasi, terroristik tarmoqlar, axborot propagandasi va mahalliy legitimlik uchun kurash AQShning yuqori texnologik harbiy salohiyatini murakkablashtirdi. Shu tariqa zamonaviy urushlarda siyosiy barqarorlik, aholi ishonchi va informatsion nazorat harbiy qudrat bilan teng darajadagi strategik omillarga aylandi.

Tadqiqot davomida axborot urushi va media manipulyatsiyasining zamonaviy gibrud mojarolardagi o'rni ham tahlil qilindi. Ijtimoiy tarmoqlar va internet platformalari zamonaviy geosiyosiy kurashning muhim vositasiga aylandi. 2016-yilgi AQSh prezidentlik saylovlari bilan bog'liq voqealar informatsion operatsiyalarning demokratik institutlarga ta'siri qanchalik kuchli bo'lishi mumkinligini ko'rsatdi. Shu bilan birga, sun'iy intellekt va deepfake

texnologiyalarining rivojlanishi informatsion xavfsizlik muammolarini yanada murakkablashtirmoqda.

Kiberurush ham gibrid mojarolarning markaziy komponentiga aylandi. SolarWinds va Colonial Pipeline bilan bog'liq hodisalar raqamli infratuzilmalar zamonaviy davlat xavfsizligining eng zaif nuqtalaridan biriga aylanganini ko'rsatdi. Shu sababli AQSh o'z milliy xavfsizlik strategiyasida kiberfazoni alohida operatsion hudud sifatida e'tirof etdi va Cyber Command faoliyatini kuchaytirdi. Bu esa XXI asr xavfsizlik muhitida texnologik ustunlik va kiberhimoya imkoniyatlari strategik ahamiyat kasb etayotganini tasdiqlaydi.

Zamonaviy geosiyosiy raqobatda gibrid urushning ahamiyati tobora ortib bormoqda. AQSh, Rossiya va Xitoy o'rtasidagi strategik qarama-qarshilik ko'proq axborot, texnologiya, iqtisodiyot va kiberfazo orqali namoyon bo'lmoqda. Ayniqsa sun'iy intellekt, yarimo'tkazgichlar va raqamli infratuzilmalar ustidan nazorat XXI asr geosiyosiy ustunligining muhim omiliga aylandi. Bu esa gibrid urushni nafaqat harbiy, balki iqtisodiy va texnologik xavfsizlik fenomeni sifatida ham talqin qilish zarurligini ko'rsatadi.

Tadqiqot natijalari shuni ko'rsatadiki, zamonaviy gibrid tahdidlarga qarshi samarali kurash faqat harbiy choralar bilan cheklanmasligi kerak. Davlat:

- axborot xavfsizligini mustahkamlashi;
- kiberhimoya tizimlarini rivojlantirishi;
- texnologik mustaqillikni ta'minlashi;
- iqtisodiy barqarorlikni saqlashi;

jamiyatning media savodxonligini oshirishi zarur bo'ladi. Ayniqsa demokratik davlatlar uchun informatsion tahdidlarga qarshi kurashda milliy xavfsizlik va so'z erkinligi o'rtasidagi muvozanatni saqlash muhim vazifa bo'lib qolmoqda.

Shunday qilib, gibrid urush XXI asr xalqaro xavfsizlik tizimining doimiy va murakkab strategik hodisasiga aylandi. Zamonaviy mojarolarning ko'p domenli xarakteri davlatlardan an'anaviy mudofaa konsepsiyalaridan tashqariga chiqib, kompleks xavfsizlik strategiyalarini ishlab chiqishni talab qilmoqda. AQSh tajribasi esa gibrid tahdidlarga qarshi kurashda texnologik, siyosiy, iqtisodiy va informatsion omillarni yagona strategik tizim sifatida ko'rish zarurligini ko'rsatmoqda.

Foydalanilgan adabiyotlar / references:

1. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies, 2007.
2. Hoffman F. G. "Hybrid Warfare and Challenges." Joint Force Quarterly. 2009. No. 52. P. 34-39.
3. Fridman O. Russian "Hybrid Warfare": Resurgence and Politicisation. London: Hurst Publishers, 2018.
4. Freedman L. The Future of War: A History. New York: PublicAffairs, 2017.
5. Murray W., Mansoor P. R. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge: Cambridge University Press, 2010.
6. Clausewitz C. On War. Princeton: Princeton University Press, 1989.
7. Sun Tzu. The Art of War. Oxford: Oxford University Press, 2013.
8. Liang Q., Xiangsui W. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House, 1999.

9. Hammes T. X. *The Sling and the Stone: On War in the 21st Century*. St. Paul: Zenith Press, 2006.
10. Singer P. W., Brooking E. T. *LikeWar: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt, 2018.
11. Rid T. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.
12. Rid T. *Cyber War Will Not Take Place*. London: Hurst Publishers, 2013.
13. Nye J. S. *The Future of Power*. New York: PublicAffairs, 2011.
14. Nye J. S. *Do Morals Matter? Presidents and Foreign Policy from FDR to Trump*. Oxford: Oxford University Press, 2020.
15. Allison G. *Destined for War: Can America and China Escape Thucydides's Trap?* Boston: Houghton Mifflin Harcourt, 2017.
16. Petraeus D., Amos J. *U.S. Army Counterinsurgency Field Manual*. Chicago: University of Chicago Press, 2007.
17. Mueller R. S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington: U.S. Department of Justice, 2019.
18. Galeotti M. "The Mythical 'Gerasimov Doctrine' and the Language of Threat." *Critical Studies on Security*. 2019. Vol. 7, No. 2. P. 157–161.
19. Stoker D., Whiteside C. "Blurred Lines: Gray-Zone Conflict and Hybrid War." *Naval War College Review*. 2020. Vol. 73, No. 1. P. 13–48.
20. Creswell J. W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Los Angeles: Sage Publications, 2018.
21. Winter C. *Documenting the Virtual "Caliphate"*. London: Quilliam Foundation, 2015.
22. U.S. Department of Defense. *National Defense Strategy of the United States of America*. Washington, 2005.
23. U.S. Department of Defense. *National Defense Strategy*. Washington, 2018.
24. U.S. Department of Defense. *2022 National Defense Strategy*. Washington, 2022.
25. U.S. Department of Defense. *Cyber Strategy Summary*. Washington, 2018.
26. U.S. Department of Homeland Security. *Countering Foreign Influence Campaigns*. Washington, 2021.
27. U.S. Department of Homeland Security. *Colonial Pipeline Cyber Incident Review*. Washington, 2021.
28. CISA. *Cybersecurity Advisories and Threat Analysis Reports*. Washington, 2022.
29. Mumford A. "Understanding Hybrid Warfare." *Cambridge Review of International Affairs*. 2020. Vol. 33, No. 6. P. 824–827.
30. Betz D. *Hybrid Conflicts and Information Warfare*. London: Lynne Rienner Publishers, 2019.