

ГИБРИД УРУШЛАРДА ҚО‘ЛЛАНИЛАДИГАН ВОСИТА ВА УСУЛЛАР

Zamonov Azizbek Avazbek-o‘g‘li

O‘zbekiston Respublikasi Jamoat xavfsizligi

universiteti magistratura tinglovchisi

Tel: +99894.046-45-45

Annotatsiya: Ushbu maqolada zamonaviy geosiyosiy muhitda keng qo‘llanilayotgan gibridd urushlarning nazariy asoslari, asosiy vositalari, taktik yondashuvlari va ularning davlatlar xavfsizligiga ta’siri tahlil qilinadi. Axborot makonini boshqarish, kiberhujumlar, iqtisodiy va diplomatik bosim, noan’anaviy harbiy operatsiyalar hamda mahalliy ijtimoiy-siyosiy jarayonlarga ta’sir o‘tkazish kabi omillar batafsil yoritiladi. Shuningdek, gibridd tahdidlarga qarshi samarali kurash mexanizmlari, milliy xavfsizlik strategiyalarini takomillashtirish bo‘yicha takliflar ishlab chiqiladi. Tadqiqot gibridd urushlarning ko‘p qatlamli, murakkab va o‘zgaruvchan xususiyatlari ortib borayotganini asoslaydi.

Kalit so‘zlar: gibridd urush, axborot tahdidlari, kiberxavfsizlik, strategik kommunikatsiya, geosiyosiy raqobat.

Аннотация: В статье рассматриваются теоретические основы, ключевые средства и тактики гибридных войн, которые становятся важным элементом современной международной безопасности. Подробно анализируются информационные операции, кибератаки, экономическое и дипломатическое давление, нетрадиционные военные действия, а также воздействие на локальные социально-политические процессы. Особое внимание уделено методам противодействия гибридным угрозам и формированию современных стратегий национальной безопасности. Исследование показывает, что гибридные угрозы имеют многослойный, динамичный и трудно прогнозируемый характер.

Ключевые слова: гибридная война, информационные угрозы, кибератаки, геополитическая конкуренция, стратегическая коммуникация.

Abstract: This article explores the theoretical foundations, major tools, and methods of hybrid warfare, which has become a critical component of the modern global security environment. It provides an in-depth analysis of information operations, cyberattacks, economic and diplomatic pressure, unconventional military tactics, and influence on local socio-political processes. Special attention is given to strategies for countering hybrid threats and improving national security policies. The study demonstrates the multilayered, dynamic, and unpredictable nature of hybrid conflicts in contemporary geopolitics.

Keywords: hybrid warfare, information threats, cyber operations, geopolitical competition, strategic communication.

Kirish

Global geosiyosiy tizimda oxirgi o'n yilliklarda kechayotgan o'zgarishlar davlatlararo raqobatning murakkab shakllarini yuzaga keltirdi. An'anaviy harbiy to'qnashuvlar o'rnini tobora ko'proq iqtisodiy, axboriy, diplomatik, kiber va ijtimoiy bosimlar bilan uyg'unlashgan gibrid urushlar egallay boshladi. Bunday strategiyalar ko'pincha aniq chegaralarga ega bo'lmaydi, ochiq harbiy agressiya tarzida namoyon bo'lmasdan, raqib davlatning ichki barqarorligiga bevosita va bilvosita ta'sir ko'rsatadi. Dunyoning turli hududlarida sodir bo'layotgan voqealar gibrid urushlarning yangi davr global xavfsizlik muhitini shakllantirayotganini ko'rsatmoqda.

Асосий қисм.

1. Гибрид уруш тushunchasi va uning rivojlanish omillari

Гибрид уруш — bu harbiy va noharbiy vositalarning muvofiqlashtirilgan tarzda qo'llanishi bo'lib, uning asosiy maqsadi raqib davlatni siyosiy, iqtisodiy, axboriy va harbiy jihatdan izdan chiqarishdan iborat. Гибрид урушlar ko'p qirrali, moslashuvchan strategiyalar bilan ajralib turadi.[1]

Гибрид уруш konsepsiyasining shakllanishiga quyidagi omillar sabab bo'lgan:

- texnologiyalarning tez rivojlanishi;
- kiberinfratuzilmaning global ahamiyat kasb etishi;
- axborot iste'molining keskin oshishi;

- iqtisodiy o‘zaro bog‘liqlikning kuchayishi;
- nodavlat aktorlarning nufuzining ortishi.

2. Gibrud urushlarning asosiy vosita va usullari

2.1. Axborot operatsiyalari va kognitiv ta’sir

Axborot makonini egallash — gibrud urushning asosiy komponenti. Bu jarayonda:

- dezinformatsiya,
- feyk yangiliklar yaratish,
- raqamli botlar orqali ijtimoiy tarmoqlarda manipulyatsiya,
- psixologik operatsiyalar,
- xalqaro axborot maydonida imijni buzish kabi usullar qo‘llanadi. Axborot operatsiyalarining asosiy maqsadi-raqibning ijtimoiy birligini zaiflashtirish, ishonch inqirozini yuzaga keltirish hamda jamoatchilik fikrini nazorat qilish.

2.2. Kiberhujumlar

Kiberhujumlar gibrud tahdidlarning eng xavfli turlaridan biri bo‘lib, davlat infratuzilmasini izdan chiqarishga qaratilgan:

- energetika tizimlariga bostirib kirish,
- bank va moliya tizimlarini ishdan chiqarish,
- hukumat axborot bazalariga zarar yetkazish,
- kiberjosuslik faoliyati kabi yo‘nalishlar mavjud. Zamonaviy kiber qurollarning qisqa vaqtda katta zarar yetkazish qobiliyati ularni strategik vositaga aylantirgan.

2.3. Iqtisodiy bosim va geoiqtisodiy kurash

Gibrud urushda iqtisodiy vositalar juda muhim:

- sanksiyalar,
- import/eksport cheklovlari,
- energiya resurslarini qurol sifatida qo‘llash,
- valyuta manipulyatsiyasi,

- investitsiyalarni siyosiy maqsadlarda cheklash. Bu usullar davlatning iqtisodiy barqarorligini zaiflashtiradi va ichki siyosiy jarayonlarga bosim o'tkazadi.

2.4. Diplomatik strategiyalar

Diplomatik bosim orqali:

- xalqaro maydonda raqibni izolyatsiya qilish,
- ittifoqlarni parchalash,
- siyosiy nufuzni pasaytirish,
- davlatning global imijiga putur yetkazish kabi maqsadlarga erishiladi.

2.5. Noan'anaviy harbiy taktika

Gibrid urushning harbiy elementi quyidagilarni o'z ichiga oladi:

- yashirin operatsiyalar,
- kontrakt jangchilar (private military companies),
- maxsus kuchlar faoliyati,
- mahalliy qurolli tuzilmalarga yordam ko'rsatish,
- chegara hududlarda kichik miqyosli provokatsiyalar.

2.6. Ijtimoiy-siyosiy jarayonlarga aralashuv

Bu usul raqib davlatning ichki barqarorligiga bevosita zarar yetkazishni ko'zlaydi:

- ichki siyosiy guruhlarini moliyalashtirish,
- etnik yoki diniy ziddiyatlarni kuchaytirish,
- saylov jarayonlariga aralashuv,
- jamoatchilik noroziligini sun'iy ravishda oshirish. [2]

3. Gibrid tahdidlarga qarshi kurash mexanizmlari

3.1. Kiberxavfsizlikni mustahkamlash

Axborot tizimlari himoyasini kuchaytirish, xalqaro kiber hamkorlikni rivojlantirish, davlat va xususiy sektorlar o'rtasida axborot almashinuvini yo'lga qo'yish talab etiladi. [3]

3.2. Axborot makonini himoya qilish

- feyk xabarlarini aniqlaydigan tizimlar yaratish,
- ommaviy axborot vositalarining mas'uliyatini oshirish,
- mediasavodxonlikni kuchaytirish,
- strategik kommunikatsiya markazlari tashkil etish.

3.3. Iqtisodiy barqarorlikni mustahkamlash

Davlat milliy iqtisodiyotini diversifikatsiya qilishi, sanksiyalarga chidamli tarmoqlarni rivojlantirishi zarur.

3.4. Diplomatik faollik

Ko'p tomonlama tashkilotlar bilan hamkorlikni kuchaytirish va xalqaro maydonda faol pozitsiyani egallash gibridd tahdidlarga qarshi himoyani mustahkamlaydi.[4]

3.5. Jamiyat barqarorligini oshirish

Aholining siyosiy, iqtisodiy va ijtimoiy ongini mustahkamlash-gibridd urushlarga qarshi eng kuchli vositalardan biridir.

Xulosa

Gibridd urushlar zamonaviy dunyoda keng ko'lamli xavf sifatida yuzaga chiqmoqda. Ularning murakkab tarkibi, ko'p qatlamli vosita va usullari davlatlarning milliy xavfsizlik siyosatini tubdan yangilashni taqozo etadi. Kiberxavfsizlik, axborot makonining barqarorligi, iqtisodiy chidamlilik va diplomatik faollik gibridd tahdidlarga qarshi kurashning asosiy poydevorini tashkil etadi.

ILMIY ADABIYOTLAR RO'YXATI

1. Galeotti, M. **The Weaponization of Everything: A Field Guide to the New Way of War**. Yale University Press, 2022.
2. NATO Cooperative Cyber Defence Centre of Excellence. **Hybrid Threats and Their Impact on Security**. Tallinn, 2020.
3. Barno, D., Bensahel, N. **The Evolution of Hybrid Warfare in the 21st Century**. War on the Rocks, 2015.
4. Wither, J. K. **Making Sense of Hybrid Warfare**. Connections: The Quarterly Journal, 2016.

5. Freedman, L. **The Future of War: A History**. Penguin Books, 2017.
6. Pomerantsev, P. **Nothing Is True and Everything Is Possible**. PublicAffairs, 2014 (axborot manipulyatsiyasi bo'yicha).
7. U.S. Army Special Operations Command. **SOF Support to Political Warfare**. White Paper, 2015.