UOT 327

KİBERTƏHLÜKƏSİZLİYİN REALİZM VƏ NEOREALİZM NƏZƏRİYYƏLƏRİ KONTEKSTİNDƏ TƏHLİLİ

Kəmilə CABBAROVA*

Məqalə redaksiyaya daxil olmuşdur: 24 aprel 2025; çapa qəbul edilmişdir: 5 may 2025; online-da çap edilmişdir: 15 may 2025.

Received: 24th of April, 2025; accepted: 5th of May, 2025; published online: 15th of May, 2025.

Açar sözlər: *realizm, neorealizm, kibertəhlükəsizlik, nəzəriyyə, dövlət, güc mübarizəsi*

Giriş

Kibernetik məkanın müasir beynəlxalq münasibətlərdə getdikcə daha da əhəmiyyətli və mürəkkəb bir sahəyə çevrilməsi ilə birlikdə, dövlətlərin və digər aktorların bu yeni sahədəki davranışlarını anlamaq üçün müxtəlif nəzəri çərçivələr təqdim olunur. Beynəlxalq münasibətlər elminin əsas təməl daşlarından olan realizm və neorealizm nəzəriyyələri, dövlətlərin anarxik bir sistemdə sağ qalma və güclərini maksimum dərəcədə artırmaq axtarışlarına diqqət yetirərək, kibertəhlükəsizlik fenomenini təhlil etmək üçün dəyərli perspektivlər təqdim edir. Bu məqalə, realizm və neorealizmin əsas fərziyyələrini və kibertəhlükəsizlik sahəsinə necə tətbiq oluna biləcəyini araşdıraraq, dövlətlərin kiberməkandakı rəqabətçi və təhlükəsizlik yönümlü davranışlarını anlamağa yönəlmiş bir çərçivə təqdim etməyi hədəfləyir. Realizmin güc balansı, təhlükəsizlik dilemması və özözünə kömək kimi əsas anlayışları ilə neorealizmin sistemik quruluşa vurğusu, dövlətlərin kibertəhdidlərə qarşı gördükləri tədbirləri, kiber silahlanma yarışını və beynəlxalq əməkdaşlıq səylərini təhlil etmək üçün kritik bir baxış bucağı təqdim edir. Bu kontekstdə, araşdırma bu iki nəzəriyyənin kibertəhlükəsizlik sahəsindəki izah gücünü qiymətləndirərək, müasir dövrün mürəkkəb kibertəhlükəsizlik mühitini anlamaq üçün təqdim etdikləri töhfələri müzakirə edəcək.

1. Kibertəhlükəsizliyin siyasi aspektlərinə nəzəri yanaşmalar

Beynəlxalq münasibətlərin əsas mövzusu dövlətlərarası qarşılıqlı siyasi fəaliyyətin səbəbləri və formalarıdır. Müharibə, sülh, sərhədlər və güc bu münasibətlərin əsas paradiqmalarını təşkil edir. Texnologiyanın sürətli inkişafı isə beynəlxalq münasibətlərin həm siyasi, həm də hərbi aspektlərində köklü dəyişikliklərə səbəb olmuşdur (4, s. 346). Bu dəyişikliklərin nəticəsində "rəqəmsal çağ təhlükəsizliyi" anlayışı formalaşmış və ənənəvi yanaşmaların yerinə daha kompleks və çoxşaxəli modellərin tətbiqinə ehtiyac yaranmışdır (7, s.86).

1991-ci ildən etibarən internetin geniş ictimai istifadəyə açılması dövlətlər, cəmiyyətlər və beynəlxalq sistemin digər aktorları arasında əlaqələrin intensivləşməsinə səbəb olmuşdur. Bu texnologiya təkcə kommunikasiya vasitəsi kimi deyil, eyni zamanda beynəlxalq proseslərin katalizatoruna çevrilmiş, informasiya axınının sürəti və miqyası ciddi

* *doktorant, AR Prezidenti yanında Dövlət İdarəçilikAkademiyası*
e-mail: kamila.jabbarov@gmail.com
https://doi.org/10.30546/25194011.2025.14.2.1056

şəkildə artmışdır. 1991-ci il Körfəz müharibəsinin media və internet vasitəsilə canlı yayımlanması, yeni informasiya dövrünün dinamikasını ortaya qoyaraq, beynəlxalq münasibətlərdə kibertəhlükəsizlik məsələsinin aktuallığını gücləndirmiş (2, s. 207) kibertəhlükəsizlik, beynəlxalq münasibətlərin əsas istiqamətlərindən biri kimi formalaşmağa başlamış və qlobal təhlükəsizlik gündəminin ayrılmaz tərkib hissəsinə çevrilmişdir. Bu proses, dövlətlərin informasiya texnologiyalarına artan asılılığını və kiberməkanın strateji əhəmiyyətini daha da ön plana çıxarmışdır.

Kibertəhlükəsizlik informasiya texnologiyaları və rəqəmsal infrastrukturun müxtəlif növ təhdidlərdən qorunması ilə bağlı fəaliyyətlərin kompleksidir. Bu təhdidlərə kiberhücumlar, məlumat sızmaları, dövlət və qeyri-dövlət aktorların apardığı kibermüharibələr və dezinformasiya kompaniyaları daxildir. Bu baxımdan, kibertəhlükəsizliyin siyasi aspektləri beynəlxalq münasibətlər nəzəriyyələrinin çoxşaxəli yanaşmaları vasitəsilə təhlil olunmaqla, həm nəzəri, həm də praktik səviyyədə əhatəli tədqiqatlara zəmin yaradır.

Texnoloji tərəqqi beynəlxalq aktorların müharibə strategiyalarına ciddi təsir göstərmiş, xüsusilə kiberməkanın inkişafı müharibə anlayışlarını və hüquqi çərçivələri yenidən nəzərdən keçirməyi zəruri etmişdir. Bu sahədə ABŞ-da dövlət və özəl sektor arasında əməkdaşlıq nəticəsində kibertəhlükəsizlik sahəsində yeni nəzəri yanaşmalar inkişaf etdirilmiş və bu sahənin konseptual əsasları gücləndirilmişdir.

Kiberməkanın zaman və məkan məhdudiyyətlərini aşması, baş verən hücumların hüquqi və siyasi statusunu mübahisəli etmişdir. Beynəlxalq hüquq, xüsusilə beynəlxalq humanitar hüquq (IHL), yeni müharibə formaları ilə bağlı qeyri-müəyyənliklər yaradır. Məsələn, beynəlxalq müharibə cinayətlərinin tərifi və tətbiqi məsələləri hələ də mübahisəlidir. Bundan əlavə, kiberməkanın dövlətlərin suverenliyini pozması və qeyri-müdaxilə prinsipini pozması məsələləri də beynəlxalq hüquqda müzakirə mövzusudur.

ABŞ-da dövlət və özəl sektor arasında kibertəhlükəsizlik sahəsində əməkdaşlıq, kiberməkanın təhlükəsizlik məsələlərinə yeni yanaşmaların inkişafına səbəb olmuşdur. Məsələn, 2015-ci ildə qəbul edilən Kibertəhlükəsizlik Məlumatlarının Paylaşılması Aktı (CISA), özəl sektorla məlumat paylaşımını təşviq etmişdir. Bundan əlavə, 2021-ci ildə Prezident Co Baydenin imzaladığı milli təhlükəsizlik memorandumunda, kritik infrastrukturun qorunması və özəl sektorla əməkdaşlığın gücləndirilməsi məqsəd qoyulmuşdur (13).

Kiberməkanın müharibə anlayışlarına təsiri, yeni nəzəri yanaşmaların inkişafına səbəb olmuşdur. Tallinn Manualı, kibermüharibə və beynəlxalq hüquq arasındakı əlaqələri araşdıran və kibermüharibənin hüquqi tərifini təqdim edən bir sənəddir. Bu sənəd, kibermüharibənin beynəlxalq hüquq çərçivəsində necə qiymətləndirilməsi və tətbiq olunması məsələlərini müzakirə edir (12).

Texnoloji tərəqqi və kiberməkanın inkişafı, beynəlxalq müharibə anlayışlarını və hüquqi çərçivələri yenidən nəzərdən keçirməyi zəruri etmişdir. ABŞ-da dövlət və özəl sektor arasında əməkdaşlıq, kibertəhlükəsizlik sahəsində yeni nəzəri yanaşmaların inkişafına və bu sahənin konseptual əsaslarının gücləndirilməsinə səbəb olmuşdur.

Bu gün, korporasiyalar, hökumətlər və fərdi şəxslər müxtəlif səviyyələrdə yerli və xarici aktorlar tərəfindən həyata keçirilən kibertəhlükələrə məruz qalır, kiberhücumlar nəticəsində dövlət və ya özəl sektora məxsus sistemlər sıradan çıxarılır və ya fəaliyyət qabiliyyəti zəiflədilir. Nümunə olaraq, 2008-ci ildə Rusiya tərəfindən Gürcüstana qarşı həyata keçirilmiş DDoS hücumları göstərilə bilər (5, s.328). Bu proseslərin təsiri ilə klassik güc anlayışı dəyişmiş, gücün müxtəlif formalarla proyeksiyası mümkün olmuşdur. Beynəlxalq münasibətlərin aktorları arasındakı rəqabət artıq texnoloji platformaya daşınmış, bu isə nəzəri yanaşmaların da yeni reallıqlara uyğun olaraq transformasiyasını zəruri etmişdir.

XXI əsrdə rəqəmsal texnologiyaların sürətli inkişafı və onların ictimai-siyasi sistemlərə nüfuzu, dövlətlərin təhlükəsizlik siyasətində kiberməkanın qorunmasını prioritet

məsələ halına gətirmişdir. Nəticədə kibertəhlükəsizlik yalnız texnoloji deyil, həm də siyasi, iqtisadi və sosial aspektləri əhatə edən kompleks bir sahəyə çevrilmişdir. Bu sahədəki proseslər dövlətlərin strateji maraqları ilə sıx şəkildə bağlıdır və mövcud beynəlxalq rəqabət mühitində kiberməkana münasibət daha çox beynəlxalq münasibətlər nəzəriyyələri çərçivəsində analiz olunmağa başlanmışdır.

Beləliklə, kiberməkan bu gün beynəlxalq münasibətlərin formalaşdığı, dövlət maraqlarının toqquşduğu və strateji rəqabətin intensivləşdiyi əsas sahələrdən birinə çevrilmişdir. Bu səbəbdən, kibertəhlükəsizlik sahəsindəki nəzəri və metodoloji yanaşmaların siyasi kontekstdə təhlili, həm elmi, həm də praktiki baxımdan böyük əhəmiyyət kəsb edir. Tədqiqat çərçivəsində bu yanaşmalardan istifadə edərək beynəlxalq sistemdə kibertəhlükələrin mahiyyətini, aktorların davranış modellərini və təhlükəsizliyin təmin olunması yollarını daha dərindən analiz etməyə çalışmışıq. Bu kontekstdə beynəlxalq münasibətlərin klassik və müasir nəzəriyyələri – realizm, neorealizm, liberalizm və konstruktivizm – kibertəhlükəsizliyin siyasi aspektlərini təhlil etmək üçün əsas konseptual çərçivələr kimi çıxış edir.

2. Realizm nəzəriyyəsi kontekstində kibertəhlükəsizlik: güc, maraqlar və anarxik sistemdə yeni məkan

Realizm nəzəriyyəsi dövlətlərin davranışlarını güc və maraqlar prizmasından izah edən əsas yanaşmalardan biridir (5). Realizmə görə, beynəlxalq əməkdaşlıq məhduddur və dövlətlər arasındakı rəqabət daimi xarakter daşıyır. Realizm kibertəhlükəsizliyi dövlətin *milli* təhlükəsizliyinin və suverenliyinin qorunması prizmasından dəyərləndirir, öz maraqlarını qorumaq üçün müdafiə qabiliyyətlərini artırır, müxtəlif müdafiə mexanizmləri qurur, ofensiv və defansiv kiber strateqiyalar hazırlayır (Məsələn, ABŞ-ın "Cyber Command" və ya Rusiyanın "kiberqoşunları" yanaşması). Realizmdə əsas müzakirə mövzusu gücün hərbi gücdən daha geniş bir anlayış kimi qəbul edilməsidir. Hərbi ünsürləri ilə gücə önəm verilməsi və varlıq mübarizəsində bütövlük kiberhücumlar və onların imkanları baxımından sırf xüsusiyyətdir.

Realist nəzəriyyəyə görə, beynəlxalq sistem anarxikdir, yəni heç bir mərkəzi hakimiyyətin və ya qlobal idarəetmənin olmadığı bir mühitdə dövlətlər bu məkan üzərində nəzarəti gücləndirmək üçün həm müdafiə, həm də hücum qabiliyyətlərini inkişaf etdirirlər. Kiberməkan da bu anarxik mühitin bir hissəsidir. Qlobal miqyasda effektiv tənzimləyici strukturların olmaması, kibertəhlükəsizliyi beynəlxalq münasibətlərdə bir güc mübarizəsi halına gətirir.

Hibrid müharibə strategiyası realizmin təhlükəsizlik və güc yanaşmasına uyğun gəlir. Burada kibermüdaxilə, informasiya müharibəsi və sosial media manipulyasiyası hərbi vasitələrlə birlikdə istifadə olunur. Kibertəhlükəsizlik məsələləri, dövlətlərin həm özlərini, həm də müttəfiqlərini qorumağa çalışdığı zaman hibrid müharibənin bir komponentinə çevrilir. Bu, kiberhücumların hərbi güc nümayiş etdirmək və ya başqa dövlətlərin daxili işlərinə müdaxilə etmək məqsədilə istifadə edilə biləcəyini göstərir. Rusiya-Ukrayna müharibəsində Rusiya tərəfindən həyata keçirilən kiberhücumlar bu modelə nümunədir.

Realizmə görə, beynəlxalq münasibətlərdə hüquqdan daha çox dövlətlərin real gücü və maraqları əsasdır. Bu səbəbdən, dövlətlər kiberməkan daxilində beynəlxalq hüququ pozmaq bahasına da olsa öz maraqlarını müdafiə edə bilərlər (3). Kibertəhlükəsizlik baxımından bu, dövlətlərin kiberməkanda öz maraqlarını qorumaq üçün hüquqi və diplomatik məhdudiyyətləri aşabiləcəklərini göstərir. Kiberhücumlar, dövlətlər tərəfindən beynəlxalq hüququ pozan bir vasitə olaraq görülə bilər. Realistlər, beynəlxalq hüququn kiberməkanla əlaqədar məsələlərə yetərli şəkildə tətbiq oluna bilməyəcəyini və bunun nəticəsində güc balansının dəyişəcəyini vurğulayırlar.

Dövlətlər, kiberməkan üzərində hegemonluq qurmağa çalışırlar, çünki bu, onlara güc və nüfuz qazandırır. Realistlər, hegemonluq istəyən dövlətlərin kiberməkan üzərindəki hərəkətlərini diqqətlə izləyirlər. Məsələn, böyük dövlətlər (ABŞ, Çin, Rusiya) kibertəhlükəsizlik sahəsində özləri üçün üstünlüklər yaratmaq və digər dövlətləri kiberhücumlarla zəiflətmək məqsədini güdürlər.

3. Tənqidi yanaşmalar və realizmin məhdudiyyətləri

Realizm nəzəriyyəsinə qarşı yönəlmiş əsas tənqidlərdən biri, realistlərin beynəlxalq münasibətlərdə dövləti vahid və bütöv bir aktor kimi qəbul etməsi, hərbi gücü isə milli maraqların qorunmasında əsas prioritet vasitə hesab etməsi ilə bağlıdır. Bu baxımdan, dövlətlər anarxik beynəlxalq sistemdə sağ qalmaq üçün güc balansına və deterrens strategiyalarına üstünlük verirlər. Lakin kiberməkanda baş verən proseslər bu klassik yanaşmanı ciddi şəkildə sarsıdır. Bu yanaşma, dövlət daxilindəki dinamikaların və müxtəlif aktorların rolunu nəzərdən qaçırır. Kibertəhlükəsizlik sahəsində isə bu yanaşma, xüsusilə natamam qalır, çünki kiberhücumlar və onlara qarşı mübarizə yalnız dövlətlərarası münasibətlərlə izah oluna bilməz. Burada informasiya, texnologiya infrastrukturu, hücum və müdafiə qabiliyyətləri, eləcə də hüquqi və etik çərçivələr ön plana çıxır. Kiberhücumlar çox vaxt dövlət aktorları tərəfindən həyata keçirilsə də, qeyri-dövlət aktorları (haker qrupları, fərdi cinayətkarlar, terror təşkilatları və s.) da bu məkanın əsas iştirakçılarındandır. Bu isə klassik realizmin dövlət mərkəzli güc modelinə ziddir.

Əlavə olaraq, kiberməkanda hücumlar tez-tez anonim, asimmetrik və hüquqi boşluqlarla dolu şəraitdə baş verir. Məsələn, bir dövlətə qarşı həyata keçirilmiş bir kiberhücumun mənşəyini dəqiq müəyyənləşdirmək çətin ola bilər. Bu isə "cəzalandırıcı cavab" və ya "güc balansı" kimi realist yanaşmaların tətbiqini əngəlləyir. Bu səbəbdən kibertəhlükəsizliklə bağlı analizlər yalnız gücə əsaslanan paradiqmalarla deyil, daha kompleks, çoxsəviyyəli və çoxaktorlu yanaşmalarla aparılmalıdır. Liberal nəzəriyyənin beynəlxalq əməkdaşlığa, konstruktivist yanaşmanın isə identiklik və normativ strukturlara vurğu etməsi, kiberməkanda baş verən prosesləri izah etmək üçün daha uyğun çərçivələr təqdim edə bilər.

Kibertəhlükəsizlik məsələləri, həmçinin beynəlxalq əməkdaşlıq və qlobal təhlükəsizlik məsələlərini əhatə edir. Kibertəhlükəsizlik, qlobal təhlükəsizliyə təsir edə biləcək bir çox tərəfi özündə birləşdirir. Ancaq realist yanaşma, dövlətlər arasındakı rəqabət və kiberməkan üzərindəki hegemonluq mübarizəsinin qlobal əməkdaşlığı əngəllədiyini irəli sürür. Əməkdaşlıq məsələsində pessimist mövqe tutan realist yanaşmaya görə, təhlükəsizlik yalnız güclərin balanslaşdırılması ilə əldə oluna bilər. Bu baxımdan, hegemon bir dövlətin rəhbərlik etdiyi sistemdə uzunmüddətli və səmərəli beynəlxalq əməkdaşlıq imkanları məhduddur. Kibertəhlükəsizlik mühitində isə hücum edən tərəfin kimliyinin məlum olmaması, dövlətlərin qeyri-qanuni strukturlarla işləməsi və informasiya asimmetriyası kimi amillər realist yanaşmanı daha da çətinləşdirir (14, s.449).

Realistlər hesab edir ki, beynəlxalq əməkdaşlığın qarşısını alan əsas amil dövlətlərin digərindən daha çox qazanc əldə etmə ehtimalı qarşısında yaranan inamsızlıqdır (3, s. 247). Yəni, Morgentaunun qeyd etdiyi kimi, "böyük güc" olan ABŞ-ın öz maraqlarını maksimuma çatdırmaq üçün atdığı addımlar beynəlxalq ictimaiyyətdə inamsızlıq yaradaraq səmimi əməkdaşlığın qarşısını alır.

Bununla yanaşı, realizmin təhlil səviyyələrindən biri olan "insan qrupları" yanaşması kibertəhlükəsizlik kontekstində müəyyən oxşarlıqlar da təqdim edir. Realist perspektivdə dövlətlərarası səviyyə ilə kiberməkanın struktur xüsusiyyətləri arasında qismən uyğunluq müşahidə olunur. Təhlilin fərdi səviyyəsinə daha yaxın olan rasionalist yanaşma isə, xüsusilə fərdi aktorların və qeyri-dövlət subyektlərinin önəm daşıdığı kibertəhlükəsizlik kontekstində daha uyğun görünür.

Beynəlxalq əlaqələrə dair üç əhəmiyyətli paradigma

Cədvəl 1

	Siyasi düşüncə strukturları	**Təhlilin ilkin səviyyəsi**	**İzahedici elementlər**	**Mövzu və ya Fokus**	**İdeoloji ənənə**
Realizm (gerçəklik)	*İnsan qrupları*	*Dövlətlərarası səviyyə*	*Hərbi güc balansı*	*Münaqişə və sifariş mühiti (anarxik beynəlxalq sistem)*	*Mühafizəkarlıq*
Rasionalizm	*Rasional aktorlar*	*Fərdi səviyyə*	*Danışıqlar, maraqlar*	*Rasional əməkdaşlıq*	*Liberalizm*
İnqilabçılıq	*Kapitalist sistemə tənqidi yanaşma*	*Qlobal sistem səviyyəsi*	*Struktur gücü və iqtisadi asılılıqlar*	*İqtisadi inkişaf və qeyri-bərabərlik*	*Radikalizm*

Bu cədvəl, beynəlxalq əlaqələrin üç əsas nəzəri paradiqmasını müxtəlif meyarlar əsasında müqayisə edir və onların əsas xüsusiyyətlərini ortaya qoyur. Cədvəldəki meyarlar və onların hər paradigmada necə təzahür etdiyi bizə bu nəzəriyyələrin beynəlxalq münasibətləri necə izah etdiyini başa düşməyə kömək edir.

Realizmdə kibertəhlükəsizlik əsasən dövlətlərin güc siyasətinə və təhlükəsizlik dilemmasına fokuslanır. Bu yanaşma kibertəhlükəsizlik kimi yeni və qeyri-ənənəvi təhlükələrə tam uyğun gəlməyə bilər, çünki kibermühitdə aktorlar yalnız dövlətlər deyil, güc anlayışı fərqli təzahür edir, qeyri-dövlət aktorlarını və normativ struktur dəyişikliklərini nəzərə almır. Amma yenə də kibertəhlükəsizliyin strateji mahiyyətini və beynəlxalq güc balansındakı rolunu izah etmək baxımından dəyərli nəzəri çərçivə təqdim edir.

Rasionalizm fərdi aktorların (dövlətlər, şirkətlər, hətta fərdi hakerlər) maraqlarını analiz etməyə çalışır. Fərdi səviyyənin təhlil səviyyəsi olaraq seçilməsi kibertəhlükəsizlik kontekstinə daha uyğundur. Bu sahədə təkcə dövlətlər deyil, fərdi aktorlar da əhəmiyyətli rol oynayır. İnqilabçılıq, əsasən, struktur dəyişikliklərinə və iqtisadi ədalətsizliklərə fokuslanır. Kibertəhlükəsizlik məsələlərində dolayısı ilə əhəmiyyətli ola bilər (məsələn, texnoloji asılılıq, informasiya imperiyası), lakin birbaşa uyğun gəlmir.

4. Neorealizmin nəzəri konsepti və kibertəhlükəsizliyə uyğunluğu

Müasir dövrdə informasiya texnologiyalarının sürətli inkişafı kiberməkanın beynəlxalq münasibətlərdə əhəmiyyətli bir qüvvə mərkəzinə çevrilməsinə səbəb olmuşdur. Bu yeni reallıq dövlətləri təhlükəsizlik, güc balansı və qarşılıqlı rəqabət kontekstində yeni yanaşmalar tətbiq etməyə vadar edir. Bu kontekstdə, beynəlxalq münasibətlərin strukturunu izah edən neorealist nəzəriyyə kibertəhlükəsizlik məsələlərinin təhlili üçün əhəmiyyətli nəzəri çərçivə təqdim edir.

Neorealizm Kennet N.Valts tərəfindən irəli sürülən və "struktural realizm" kimi tanınan yanaşmadır. Valtsın 1979-cu ildə nəşr olunan "Beynəlxalq Siyasətin Nəzəriyyəsi" əsəri struktural realizmin əsasını təşkil edir. Neorealizmin əsas prinsiplərinə görə beynəlxalq sistem anarxikdir, yəni mərkəzsiz və qaydasızdır, dövlətlər beynəlxalq münasibətlərin əsas aktorlarıdır, dövlətlər öz təhlükəsizliklərini təmin etmək və güc balansı yaratmaq məqsədilə hərəkət edirlər (15).

Neorealizm beynəlxalq münasibətlərdə sistem anlayışına əsaslanaraq, dövlətlərin davranışlarının beynəlxalq anarxiyanın strukturu ilə məhdudlaşdığını iddia edir. K. Valts kimi klassik neorealistlərə görə, dövlətlərin üzərində onları qoruyacaq və ya cəzalandıracaq daha yüksək bir hakimiyyət mövcud deyil. Bu vəziyyət dövlətləri qorxu və qeyri-müəyyənlik şəraitində yaşamağa, nəticədə hərbi, iqtisadi və texnoloji imkanlarını artırmağa təşviq edir (5, s. 77-78). Valts dövlətləri unitar və rasional aktorlar kimi qəbul edərək,

onların hərəkətlərini təhlükəsizlik ehtiyacları və güc axtarışı ilə izah edir. Neorealizmə görə, dövlətlər əməkdaşlıqdan çox rəqabətə üstünlük verir və öz maraqlarını qorumaqda eqoist davranırlar (3, s.248).

Müasir texnoloji inkişaf fonunda dövlətlər birbaşa hərbi toqquşmalardan çəkinərək qeyri-ənənəvi metodlara, xüsusilə, kibermünaqişə strategiyalarına – üstünlük verirlər. Bu vəziyyət neorealist yanaşmanı daha da aktuallaşdırır. Valsın qeyd etdiyi kimi, münaqişələrin səbəbləri zaman və şəraitə uyğun dəyişə bilər (15). Kibermünaqişələrin artması və informasiya təhlükəsizliyinin hərbi təhlükəsizliklə eyni səviyyədə önəm kəsb etməsi bu nəzəri müddəaya uyğun gəlir.

Neorealizmin əsas fərqləndirici xüsusiyyətlərindən biri beynəlxalq sistemdəki *etibarsızlıq* (uncertainty) mühitidir. Bu şəraitdə dövlətlərin əsas məqsədi öz suverenliklərini və təhlükəsizliklərini qorumaqdır. Klassik realizmdən fərqli olaraq, neorealizm gücü beynəlxalq siyasətin məqsədi deyil, vasitəsi kimi dəyərləndirir (1, s.46). Bu baxımdan, kibertəhlükəsizlik sahəsində çəkindirmə və hücum qabiliyyətlərinin inkişafı dövlətlərin varlığını qorumaq üçün qəbul etdiyi strategiyalar sırasına daxil olur.

Neorealizmə görə, beynəlxalq sistemdə dövlətlər öz maraqlarını təmin etmək üçün güc mübarizəsində iştirak edir və qarşılıqlı etimadın aşağı səviyyədə olması təhlükəsizlik dilemmasını dərinləşdirir. Bu çərçivədə hücum-müdafiə balansı konsepsiyası xüsusi əhəmiyyət daşıyır. Bu balans hücumun nə qədər sərfəli, müdafiənin nə qədər effektiv olduğunu müəyyən edir (5, s. 77, 355), texnologiya bu balansda əsas rol oynayır və effektiv, lakin ucuz texnologiyalar etibarsızlığa səbəb olaraq müharibə ehtimalını artırır (9).

Kibermüharibə neorealist analiz üçün əlverişli nümunədir. Kiberhücumların həyata keçirilməsi nisbətən ucuz və asan, müdafiə isə daha mürəkkəb və xərclidir. Singer və Friedman-ın araşdırmalarına əsasən, ABŞ ordusunda bir kiberhücumun dəyəri müdafiədən üç dəfə azdır. Hücum üçün zərərli proqram təminatı kifayət etdiyi halda, müdafiə üçün inkişaf etmiş proqram təminatı, güclü infrastruktur və yüksək ixtisaslı mütəxəssislər tələb olunur (6, s. 218).

Analitiklərə görə, dövlətlərin bütün milli şəbəkələrini müdafiə etməsi praktik olaraq mümkün deyil. Xüsusilə, özəl sektor tərəfindən idarə olunan enerji, nəqliyyat və bank sistemləri kimi kritik infrastrukturlar zəif həlqələr hesab olunur. Rusiya və Çin kimi ölkələrdə dövlətin internet və rəqəmsal məkan üzərində güclü nəzarəti kibermüdafiəni daha effektiv edir.

Kiberməkanda hücum üstünlüyünün digər mühüm cəhəti təcavüzkarın kimliyinin asanlıqla müəyyən edilə bilməməsidir. Kiberhücumlar istənilən yerdən və anonim şəkildə həyata keçirilə bilər. Bu, dövlətlərin cavab reaksiyalarını ləngidir və kibermühiti daha riskli edir. Lakin bütün bu üstünlüklərə baxmayaraq, neorealist yanaşmanın kiberməkanla bağlı *məhdudiyyətləri* də vardır. Birincisi, neorealizm əsas aktor kimi yalnız dövlətləri nəzərdə tutur. Halbuki, kiberməkanda fərdi hakerlər, haktivistlər, texnoloji şirkətlər kimi qeyri-dövlət aktorları da mühüm rol oynayır. Həmçinin kiçik və hərbi cəhətdən zəif dövlətlər də kiber sahədə güc nümayiş etdirə bilər. Məsələn, Şimali Koreyanın texnoloji infrastrukturu zəif olsa da, effektiv kiber döyüşçülərə və imkanlara malikdir (11, s. 28).

İkincisi, neorealizmin əsaslandığı güc balansı anlayışını kiberməkanda tətbiq etmək çətindir. Fiziki müharibədə dövlətin hərbi gücünü ölçmək mümkün olsa da, kiberməkanda bu göstəricilər qeyri-müəyyəndir və tez-tez dəyişir. Məsələn, ABŞ hərbi və iqtisadi cəhətdən güclü olmasına baxmayaraq, kiberhücumlara ən çox məruz qalan dövlətlərdən biridir (11, s. 45). Kiberməkandakı güc konfiqurasiyası gizli və asimmetrik olduğuna görə, onu ölçmək və proqnozlaşdırmaq çətindir.

Nəticə

Beləliklə, neorealist yanaşma kibermüharibənin bəzi aspektlərini – xüsusilə, dövlətlərin davranış motivasiyalarını və texnologiyanın hücum-müdafiə balansına təsirini – izah

etsə də, bu yanaşmanın qeyri-dövlət aktorların rolu və kibergücün qeyri-müəyyən təbiəti qarşısında məhdudiyyətləri qalır. Belə ki:

- Neorealistlər kiberməkanı beynəlxalq anarxiyanın bir hissəsi kimi qiymətləndirirlər. Kiberməkanda qlobal nəzarət və hüquqi çərçivə olmadığından, dövlətlər öz təhlükəsizliklərini fərdi şəkildə təmin etməyə çalışırlar.
- Kiberməkan dövlətlərə qeyri-simmetrik üstünlüklər təqdim edir. Neorealizmə görə, bu gücün əldə edilməsi dövlətin suverenliyini və strateji mövqeyini qorumaq üçün vacibdir.
- Kibertəhlükəsizlik neorealizmdə rəqabət və çəkindirmə strategiyalarının ayrılmaz hissəsidir. Hücum və cavab qabiliyyəti rəqibləri zərərli fəaliyyətlərdən çəkindirmək məqsədi daşıyır.
- Kiberhücumlar artıq müstəqil münaqişə vasitəsi deyil, hibrid müharibələrin əsas komponentlərindən birinə çevrilmişdir. Neorealistlər bunu dövlətlərin maraqlarını qorumaq üçün istifadə etdiyi yeni güc vasitəsi kimi qəbul edirlər.
- Neorealizm dövlətlərarası əməkdaşlığa skeptik yanaşır və kiberməkanda bu əməkdaşlıq adətən məhdud və taktiki xarakter daşıyır. Etimad səviyyəsinin aşağı olması isə təhlükəsizlik dilemmasını daha da gücləndirir və uzunmüddətli əməkdaşlığı çətinləşdirir.

Neorealizm, kibertəhlükəsizlik məsələlərinin beynəlxalq sistemin güc və təhlükəsizlik dinamikası çərçivəsində təhlil olunmasına imkan yaradır. Anarxik sistemdə dövlətlərin təhlükəsizlik və güc əldə etmə cəhdləri kiberməkan üzərində rəqabətin intensivləşməsinə səbəb olur. Hibrid müharibələrin və kibergüc anlayışının aktuallaşması, neorealist nəzəriyyənin bu sahədə daha geniş tətbiqinə imkan verir.

Neorealizmin struktur əsaslı yanaşması, kibertəhlükəsizlik kimi yeni, lakin strateji sahələrin təhlili üçün əlverişli nəzəri çərçivə təqdim edir. Dövlətlərin kiberməkan üzərində üstünlük və təhlükəsizlik ehtiyacları, bu yanaşmanın əsas komponentləri olan anarxik sistem, güc balansı və rasional davranış anlayışları ilə üst-üstə düşür. Beləliklə, kibertəhlükəsizlik məsələlərinin neorealist nəzəriyyə çərçivəsində izahı həm analitik, həm də praktik baxımdan səmərəli nəticələr ortaya qoyur.

ƏDƏBİYYAT

1. Bayraktar G. Siber Savaş ve Ulusal Güvenlik Stratejisi, İstanbul: Yeniyüzyıl Yayınları, 2015, 232 s.
2. Bıçakçı S. Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu// Uluslararası İlişkiler Dergisi, 2012, 9(34), s.205-226.
3. Çetinkaya Ş. Güvenlik Algılaması ve Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları // 21. Yüzyılda Sosyal Bilimler, 2012, Sayı 2, s. 241-260.
4. Knutsen T.L. Uluslararası İlişkiler Teorisi Tarihi. İstanbul: Açılım Kitap, 2006, 440 s.
5. Roskin M., Berry N. Uluslararasi İlişkiler Uİ'nin Yeni Dünyası. Ankara: Adres Yayınları, 2014, 481 s.
6. Singer P.W. ve Friedman, A., Siber Güvenlik ve Siber Savaş. Ankara: Buzdağı Yayınları, 2015, 396 p.
7. Dunn M. A. Securing The Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory//. Johan Eriksson and Giampiero Giacomello (Ed.), International Relations and Security in the Digital Age, New York: Routledge Publishing, 2007, 1, p.85-106.
8. Dunne T, Kurki, M., & Smith, S. International Relations Theories. Oxford: OUP Oxford, 2013, p.14-35.
9. Jervis R. Cooperation Under the Security Dilemma. World Politics. New York: Cambridge University Press 1978, v.30 (2), p.167-214.
10. Morgenthau H. Politics Among Nations: The Struggle for Power and Peace. New York: Alfred A. Knopf. 1948, 489 p.
11. Sanger D.E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.

New York: Crown Publishing. 2020, 348 p.
12. Schmitt M. Tallinn Manual on the International Law Applicable to Cyber Warfare. New York: Cambridge University Press, 2013, 302 p.
13. Sedenberg E.M. Dempsey J. X. Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs, 2018. URL: (https://arxiv.org/pdf/1805.12266v1).
14. Stone A. What is Supranational Constitution? An Essay in International Relations Theory // The Review of Politics, 1994, 56 (3), pp. 441-474.
15. Waltz K.N. Man, the State, and War: A Theoretical Analysis. New York: Columbia University Press. 1954, 242 p.

Резюме

Камиля Джаббарова

Анализ кибербезопасности в контексте теорий реализма и неореализма

В современном мире кибербезопасность перестала быть исключительно техническим вопросом и стала одним из центральных компонентов глобального политического управления, динамики международных отношений и общественно-политической стабильности. Для адекватного понимания этого сложного феномена теории реализма и неореализма предлагают важные аналитические рамки. Стратегические подходы государств в сфере кибербезопасности дифференцируются в зависимости от их внутренней политической структуры, положения на международной арене и спектра имеющихся технологических ресурсов.

Парадигма реализма концептуализирует международную систему как анархическую среду и постулирует, что первостепенной целью государств является императив обеспечения их суверенной безопасности. С этой точки зрения, кибербезопасность представляет собой критически важную арену, на которой государства конкурируют с целью наращивания своего силового потенциала, достижения стратегического превосходства и ограничения возможностей своих соперников. Фокус классического реализма на уровне отдельных акторов может предоставить определенные аналитические преимущества для анализа поведения государственных и негосударственных акторов в сфере кибербезопасности.

Неореализм, в свою очередь, предлагает структурно ориентированный подход к международным отношениям. Согласно этой теории, поведение государств непосредственно определяется структурой международной системы. Кибербезопасность также рассматривается как комплекс действий, предпринимаемых государствами с целью сохранения своего существующего положения в системе и увеличения своей доли в региональном и глобальном балансе сил. Неореалистическая перспектива позволяет понять, как системные ограничения и возможности влияют на стратегии государств в области кибербезопасности.

Хотя обе теории анализируют кибербезопасность как неотъемлемый элемент борьбы государств за власть, реализм подчеркивает, что государства прибегают к широкому спектру средств для обеспечения своей безопасности. Неореализм же утверждает, что такое поведение формируется именно в соответствии с императивами, порождаемыми анархической структурой международной системы. Эти аналитические подходы имеют фундаментальное значение для всестороннего понимания растущей роли и влияния кибербезопасности в международных отношениях. Тем не менее, следует отметить, что философско-методологические рамки существующих парадигм имеют определенные ограничения в полном охвате такого динамичного и быстро развивающегося феномена, как кибербезопасность. Это, в свою очередь, указывает на необходимость независимых или гибридных теоретических подходов, учитывающих специфические особенности сферы кибербезопасности. Будущие исследования в области кибербезопасности должны быть сосредоточены на таких направлениях, как взаимодействие государственных и негосударственных акторов в киберпространстве и влияние новых технологий (искусственный интеллект, блокчейн и т. д.) на кибербезопасность, что является необходимым и внесет важный вклад как в углубление теоретических знаний, так и в развитие практических применений.

Ключевые слова: *реализм, неореализм, кибербезопасность, теория, государство, борьба за власть*

Summary

Kamila Jabbarova

Analysis of Cybersecurity in the Context of Realism and Neorealism Theories

In the modern world, cybersecurity has ceased to be solely a technical issue and has become one of the central components of global political governance, the dynamics of international relations, and socio-political stability. To adequately understand this complex phenomenon, the theories of realism and neo-realism offer important analytical frameworks. States' strategic approaches in the field of cybersecurity are differentiated depending on their internal political structure, their position on the international stage, and the spectrum of technological resources they possess.

The paradigm of realism conceptualizes the international system as an anarchic environment and postulates that the primary goal of states is the imperative to ensure their sovereign security. From this perspective, cybersecurity represents a critically important arena in which states compete to build their power potential, achieve strategic superiority, and limit the capabilities of their rivals. The focus of classical realism on the level of individual actors can provide certain analytical advantages for analyzing the behavior of state and non-state actors in the field of cybersecurity.

Neorealism, in turn, offers a structurally oriented approach to international relations. According to this theory, the behavior of states is directly determined by the structure of the international system. Cyber-security is also viewed as a set of actions undertaken by states to maintain their existing position in the system and increase their share in the regional and global balance of power. The neorealist perspective allows us to understand how systemic constraints and opportunities influence states' cybersecurity strategies.

Although both theories analyze cybersecurity as an integral element of states' struggle for power, realism emphasizes that states resort to a wide range of means to ensure their security. Neorealism, on the other hand, argues that such behavior is formed precisely in accordance with the imperatives generated by the anarchic structure of the international system. These analytical approaches are of fundamental importance for a comprehensive understanding of the growing role and influence of cybersecurity in international relations. Nevertheless, it should be noted that the philosophical and methodological frameworks of existing paradigms have certain limitations in fully encompassing such a dynamic and rapidly evolving phenomenon as cybersecurity. This, in turn, indicates the necessity of independent or hybrid theoretical approaches that take into account the specific characteristics of the field of cybersecurity. Future research in the field of cybersecurity should focus on areas such as the interaction of state and non-state actors in cyberspace and the impact of new technologies (artificial intelligence, blockchain, etc.) on cybersecurity, which is necessary and will make an important contribution to both the deepening of theoretical knowledge and the development of practical applications.

Key words: *realism, neorealism, cybersecurity, theory, state, power struggle*

Baş redaktorun müavini s.e.d., prof. İbrahimova Gülzar İsaxan qızının rəyi əsasında çapa məsləhət görülmüşdür.