«ՏԵՂԵԿԱՏՎԱԿԱՆ ՊԱՏԵՐԱԶՄ» ՀԱՍԿԱՑՈՒԹՅԱՆ ՀԱՐՑԻ ՇՈՒՐՋ*

ՀՏԴ 004 DOI: 10.52063/25792652-2024.3.22-102

ԱՆՆԱ ՍԻՍՈՅԱՆ
Երևանի պետական համալսարանի
միջազգային հարաբերությունների ֆակուլտետի
քաղաքագիտության ամբիոնի հայցորդ,
ք. Երևան, Հայաստանի Հանրապետություն
anna.sisoyan@ysu.am
ORCID: 0009-0009-6170-5366

Հոդվածի նպատակն է ներկայացնել «տեղեկատվական պատերազմ» հասկացությունը և դրա բաղադրիչները՝ առանձին ուսումնասիրության առարկա դարձնելով տեղեկատվական պատերազմ, տեղեկատվական օպերացիա, տեղեկատվական դիմակայություն և տեղեկատվական գրոհ հասկացությունները, ինչպես նաև բացահայտել վերոնշյալ բաղադրիչների բովանդակային և իմաստային առնչությունները:

Նպատակին հասնելու համար հոդվածի շրջանակներում առաջադրվել են հետևյալ հետազոտական խնդիրները՝ ուսումնասիրել արևմտյան և ռուսական աղբյուրներում նշված հասկացությունների շուրջ մոտեցումները, սահմանումները, կատարել համեմատություն և վեր հանել տեղեկատվական պատերազմի բաղադրիչների արդյունավետ կիրառման նախապայմանները:

Հետազոտության ընթացքում կիրառվել են նկարագրական, համեմատական և կոնտենտ վերլուծության մեթոդները:

Հոդվածում որպես աղբյուր օգտագործվել են ինչպես մի շարք ռազմավարական փաստաթղթերում տեղ գտած, այնպես էլ ոլորտի հայտնի տեսաբանների և մասնագետների կողմից առաջ քաշված ձևակերպումներ ու մոտեցումներ:

Հոդվածի շրջանակներում դիտարկվում են նաև պետությունների արտաքին քաղաքականության իրականացման համատեքստում գրագետ տեղեկատվական պատերազմներ վարելու ժամանակակից գործիքակազմերը:

Աշխատանքի շրջանակում կատարված եզրահանգումները թույլ են տալիս պնդել, որ արդի դարաշրջանում տեղեկատվական պատերազմները վարվում են տարբեր բաղադրիչների և գործիքակազմերի կիրառմամբ, որոնց գրագետ և արդյունավետ օգտագործումը հնարավորություն է տալիս գերակայության հասնելու հակառակորդի նկատմամբ: Հայաստանի Հնարապետության դեմ այսօր վարվում է ակտիվ տեղեկատվական պատերազմ, որին դիմակայելու համար մեր երկրին անհրաժեշտ է ճիշտ տեղեկատվական քաղաքականության մշակում և իրականացում, ինչն էլ իր հերթին պահանջում է պետական մակարդակով լուրջ և համակարգված քանքեր և հետևողականություն:

Հիմնաբառեր՝ *տեղեկատվական պատերազմ, տեղեկատվական դիմակայություն, տեղեկատվական գործողություն, տեղեկատվական օպերացիա, հիբրիդային պատերազմ, կիբերտարածություն, կիբերհարձակումներ:*

* Հոդվածը ներկայացվել է 11.07.2024թ., գրախոսվել՝ 27.08.2024թ., տպագրության ընդունվել՝ 31.10.2024թ.:

ՆԵՐԱԾՈՒԹՅՈՒՆ

Արդի միջազգային հարաբերություններում պետություններն իրենց ազգային շահերը պաշտպանելու և առաջ տանելու համար հաճախ են կիրառում տեղեկատվական պատերազմի լայն գործիքակազմեր: 21-րդ դարում հատկապես, տեղեկատվական տեխնոլոգիաների զարգացմանը զուգընթաց, ի հայտ են գալիս այդ պատերազմների վարման նոր մեթոդներ ու եղանակներ: Բանն այն է, որ ներկայումս տեղեկատվական-հաղորդակցական հոսքերի արագությունն ու ինտենսիվությունը մի կողմից էականորեն հեշտացնում են տեղեկատվության հասանելիությունը հասարակության լայն շրջանակներին, մյուս կողմից առաջ են բերում նոր մարտահրավերներ և սպառնալիքներ: Այդ իսկ պատճառով կարևորվում է տեղեկատվական պատերազմների և դրա բաղադրիչների ուսումնասիրությունը՝ մի կողմից հակառակորդ կողմի իրականացրած գործողությունները նույնականացնելու և դրանց դիմագրավելու, մյուս կողմից էլ սեփական տեղեկատվական քաղաքականությունը մշակելու, գրագետ տեղեկատվական գործողություններ իրականացնելու համատեքստում:

Մեր երկրի շուրջ ստեղծված աշխարհաքաղաքական բարդ իրավիճակն ու 44-օրյա պատերազմի ժամանակահատվածում հակառակորդի կողմից կիրառված հիբրիդային պատերազմը, որն ուղեկցվում էր հստակ կազմակերպված տեղեկատվական հարձակումներով, էլ ավելի հրատապ և արդիական են դարձնում այս ուղղությամբ տարվող աշխատանքների կարևորությունը: Չնայած ՀՀ Ազգային անվտանգության ռազմավարության մեջ անդրադարձ կա տեղեկատվական անվտանգությանը, կիբերանվտանգությանն ու տեղեկատվական պատերազմներին, այնուամենայնիվ հարկ է ընդգծել, որ որոշ դրույթներ և ձևակերպումներ առաջացնում են հասկացութային խառնաշփոթ, ինչպես նաև կրում են դեկլարատիվ բնույթ: Մասնավորապես, ՀՀ Ազգային անվտանգության ռազմավարական փաստաթղթում նշվում է. «Հայաստանի տեղեկատվական անվտանգության քաղաքականության հիմնական նպատակը անհատի, հասարակության և պետության շահերի հավասարակշռումն ու պաշտպանությունն է» (ՀՀ Ազգային անվտանգության ռազմավարություն, Բաց և անվտանգ տեղեկատվական և կիբերտիրույթների ապահովում 30-31): Հաջորդիվ հիշատակվում է, որ ժամանակակից աշխարհում ավելի սուր դրսևորումներ են ստանում տեղեկատվական պատերազմները, որոնք ներառում են քարոզչության, մանիպուլյացիաների, կեղծ լուրերի և ապատեղեկատվության գործիքակազմ և հաճախ թիրախավորում են ժողովրդավարական արժեքները, և որ այդ համատեքստում պետությունը աշխատելու է հանրային իրազեկվածության և մեդիագրագիտության մակարդակի բարձրացման ուղղությամբ՝ նպատակ ունենալով հզորացնելու տեղեկատվական պատերազմներին հակազդելու հասարակության և պետության կարողությունները (ՀՀ Ազգային անվտանգության ռազմավարություն, Բաց և անվտանգ տեղեկատվական և կիբերտիրույթների ապահովում 31): Նշված փաստաթղթում տեղ գտած ձևակերպումները կարելի է դիտարկել որպես առկա խնդիրների արձանագրում, այնինչ նման պարագայում առավել նպատակահարմար և արդյունավետ կարող էր լինել առանձին տեղեկատվական ռազմավարության դոկտրինի և գործողությունների ծրագրի մշակումը, հստակ թիրախների, նպատակների, քայլերի հաջորդականության, մեթոդների և նպատակին հասնելու համար անհրաժեշտ ռեսուրսների սահմանումը:

Օրինակ՝ շատ երկրներ, այդ թվում Ռուսաստանի Դաշնությունը, ունեն տեղեկատվական անվտանգության առանձին ռազմավարական հայեցակարգ, որով սահմանվում են այդ ուղղությամբ տարվող քաղաքականության առաջնահերթությունները: Ամերիկայի Միացյալ Նահանգները և Մեծ Բրիտանիան նույնպես ունեն մի շարք օրենսդրական ակտեր, որոնցով կարգավորվում են տեղեկատվության առանձին բաղադրիչների շրջանառման, պետական, քաղաքական

և հանրային սեկտորներում տեղեկատվական հոսքերի կառավարմանն առնչվող հարցեր, ինչպես նաև ունեն ոլորտը կարգավորող համապատասխան գերատեսչություններ: Վերոնշյալ երկրների այդ հայեցակարգային փաստաթղթերում առանցքային տեղ է զբաղեցնում «տեղեկատվական պատերազմ» հասկացությունը:

Տեղեկատվական պատերազմ

Ինչպես ակադեմիական, այնպես էլ գործնական քաղաքականությամբ զբաղվող մասնագիտական շրջանակներում «տեղեկատվական պատերազմ» և հարակից այլ հասկացությունների սահմանման և կիրառման հարցերի առնչությամբ առկա են և՛ համընդհանուր ճանաչում գտած մոտեցումներ, և՛ միմյանցից էականորեն տարբերվող տեսակետներ:

Ամերիկյան հեղինակներ Վ. Հաթչինսոնը և Մ. Ուորենը նշում են, որ տեղեկատվական պատերազմների հիմնական զենքն ու թիրախը տեղեկատվությունն է: «Դա այն ապրանքն է, որը պետք է շահարկվի հօգուտ նրանց, ովքեր փորձում են ազդել իրադարձությունների վրա: Դրան հասնելու միջոցները բազմազան են: Գլխավոր դերակատարները կարող են փորձել ուղղակիորեն փոխել տվյալները կամ մրցակիցներին զրկել դրանց հասանելիությունից» (Hutchinson, Warren 1):

ԱՄՆ Օդային ուժերի դեպարտամենտի կողմից 1996 թվականին հրապարակված գրքույկում նշվում է, որ առհասարակ պատերազմը հարձակման, պաշտպանության և շահագործման մասին է, և տեղեկատվական պատերազմը չի տարբերվում դրանից, այլ խոսքերով «տեղեկատվական պատերազմը ցանկացած գործողություն է, որն ուղղված է հակառակորդի տեղեկատվության և տեղեկատվական գործառույթների մերժմանը, շահարկմանը, խափանմանը կամ ոչնչացմանը՝ պաշտպանելու համար սեփական գործողությունները» (ԱՄՆ Օդային ուժերի դեպարտամենտի գրքույկը 5):

Հասկացության շուրջ ՆԱՏՕ-ի անդրադարձում նշվում է, որ տեղեկատվական պատերազմը գործողությունների ամբողջություն է, որն իրականացվում է հակառակորդի նկատմամբ տեղեկատվական ու հոգեբանական առավելություն ձեռք բերելու համար: Այն ներառում է սեփական տեղեկատվական տարածքի վերահսկումը, սեփական տեղեկատվական հասանելիության պաշտպանությունը, ինչպես նաև հակառակորդի տեղեկատվության ձեռքբերումը և օգտագործումը, հակառակորդի տեղեկատվական համակարգերի ոչնչացումն ու տեղեկատվական հոսքերի խաթարումը (NATO Website 1):

Ռուս քաղաքագետ Ի. Պանարինը, անդրադառնալով թեմային գրում է, որ տեղեկատվական պատերազմը առաջին հերթին ըստ սեփական շահերի տեղեկատվական հոսքերի, հայտնի և անհայտ տեղեկատվության կառավարումն է՝ որոշակի արդյունքի հասնելու նպատակով: Պանարինը նաև նշում է՝ ըստ էության, տեղեկատվական պատերազմի կազմակերպիչ կարող է դառնալ ցանկացած մարդ, փոքր խումբ, բիզնես կառույց, պետություն: Իսկ այն հարցին, թե ում կողմից են նախագծվում տեղեկատվական պատերազմիի նպատակները, հեղինակը նշում է «ռեժիսոր-գաղափարախոսներին»: «Ռեժիսոր-գաղափարախոսների» հիմնական նպատակն է տեղեկատվական պատերազմի նպատակի և իմաստի ձևակերպումը (Панарин 12):

Վերջին ձևակերպումը, ընդգրկելով նախորդ ձևակերպումները իմաստային առումով, նաև անդրադառնում է տեղեկատվական պատերազմի կազմակերպիչներին և նախագծողներին: Ընդհանուր առմամբ, տեղեկատվական պատերազմը կարելի է սահմանել որպես հակամարտություն, որտեղ զենքի փոխարեն կիրառվում է տեղեկատվությունը: Վերոնշյալ սահմանումներում ընդգծվում է տեղեկատվական պատերազմների ընթացքում սեփական տվյալներն ու տեղեկատվական տարածքը պաշտպանելու կարևորությունը և տեղեկատվական առումով հակառակորդին

խոցելի դարձնելը: Այս իմաստով ենթադրվում է, որ տեղեկատվական պատերազմները և՛ պաշտպանողական, և՛ հարձակողական տիպի գործողություններ են:

Օրինակ, Ա. Իվանցովը շեշտը դնում է տեղեկատվական պատերազմի հարձակողական կողմի վրա՝ նշելով, որ տեղեկատվական պատերազմը կազմակերպված պայքար է, որը ունի ագրեսիվ և ինտենսիվ բնույթ: Տեղեկատվական տարածքում պատերազմներ իրականացնելու համար կիրառվում են այնպիսի ագրեսիվ տեխնոլոգիաներ, ինչպիսիք են լայնածավալ տեղեկատվական արշավները, վարկաբեկող PR ակցիաները, քարոզչությունը և այլն (Иванцов 30):

Ըստ նրա՝ տեղեկատվական պատերազմը ոչ այլ ինչ է, քան համակարգերի բացահայտ և թաքուն նպատակաուղղված գործողություններ, որոնց նպատակն է ստանալ առավելություն նյութական ոլորտում (Иванцов 32):

Այն հարցին, թե ինչ կերպ տեղեկատվությունը կարող է շահարկվել, անդրադարձ է կատարվում Դ. Վենտրեի աշխատության մեջ: Հեղինակը նշում է, որ տեղեկատվական պատերազմը կարող է իրականացվել հոգեբանական գործողությունների, էլեկտրոնային պայքարի, ռազմական խորամանկության, օպերացիոն անվտանգության և հակառակորդի տեղեկատվական անվտանգության խաթարման, ինչպես նաև համակարգչային ցանցի գրոհների միջոցով (Ventre 44): Նշված ցանկին կարելի է հավելել այլ բաղադրիչներ ևս, ինչպես օրինակ, մամուլի հետ տարվող աշխատանքը, լոբբինգը, հովանավորչական աշխատանքը և այլն: Հակիրճ անդրադառնանք Վենտրեի առաջ քաշած բաղադրիչներից յուրաքանչյուրին:

Հոգեբանական գործողություններ

Գործողության այս տեսակը կարելի է սահմանել որպես այնպիսի հաղորդակցության կիրառում, որը ազդում է վարքագծի վրա:

Գործողության այս տեսակը ի հայտ է եկել մինչ թվային դարաշրջանը և հավանաբար դեռ երկար կմնա գործածության մեջ: Հաղորդակցումը հարաբերությունների ստեղծման միջոց է, որն ընդգրկում է՝

• լրատվամիջոցների վերահսկումը՝ ստացվող և հեռարձակող տեղեկատվությունը կարգավորելու նպատակով,

• տեղեկատվության միջոցով ուղեղների մանիպուլյացիան,

• բառերի, պատկերների, ելույթների կամ ձայնի օգնությամբ հուզական ազդեցության օգտագործումը,

• սեփական քարոզչական արշավները որպես դրական, իսկ հակառակորդինը որպես բացասական ներկայացելը,

հոգեբանական գործողությունների կիրառումը պահանջում է հաղորդակցության և ինֆորմացիոն տեսությունների, անհատների հոգեբանության, նրանց վարքագծի և մշակույթի մասին խորը գիտելիքներ:

Էլեկտրոնային պայքար

Էլեկտրոնային պայքարը կարևորում է ծառայությունների խաթարումը, խորամանկությունը (ուղղված մարդկանց կամ ավտոմատացված համակարգերին) և հակառակորդի էլեկտրոնային համակարգերից անհրաժեշտ տեղեկատվության դուրսբերումն ու շահարկումը:

Էլեկտրոնային պայքարի նպատակը էլեկտրոմագնիսական սպեկտրի կառավարումն է:

Դրա բաղադրիչներն են՝

• էլեկտրոնային գրոհը՝ ուղղված մարդկանց, սարքավորումներին ու կայանքներին, խաթարելու նրանց աշխատանքը,

• էլեկտրոնային պաշտպանությունը, որը ներառում է համակարգերի ապահովումը հակառակորդի հնարավոր գրոհներից: Էլեկտրոնային պաշտպանության կարևոր բաղադրիչներից է գաղտնագրումը,

• Էլեկտրոնային պայքարը նաև աջակցում է էլեկտրամագնիսական էներգիայի աղբյուրների որոնմանը, հայտնաբերմանը, նույնականացմանն ու խաթարմանը՝ անմիջական վտանգները չեզոքացնելու համար:

Ռազմական խորամանկություն

Ռազմական խորամանկությունը պատերազմի ժամանակ ռազմական միավորի կողմից կիրառվող գործողությունների համալիր է, որը միտված է հակառակորդին մոլորեցնելու միջոցով բարենպաստ պայմաններ ստեղծելուն: Այն կարող է արվել տեսողական, ինֆորմացիոն խաբկանքի միջոցով կամ հակառակորդի շրջանում ապատեղեկատվության տարածմամբ: Այն սերտ առնչություն ունի գործառնական անվտանգության հետ, քանի որ գործառնական անվտանգությունը փորձում է թաքցնել տեղեկատվությունը սեփական ռազմական կարողության, սպասվող և ձեռնարկվելիք գործողությունների վերաբերյալ, կամ հակառակորդին հասցնել այնպիսի տեղեկատվություն, որը կարող է մոլորեցնել:

Տեղեկատվական անվտանգություն

Այս հասկացությունը պարունակում է այն միջոցները, որոնք պաշտպանում են տեղեկատվությունը և տեղեկատվական համակարգերը՝ ապահովելով դրանց հասանելիությունը, ամբողջականությունը, վավերությունը, գաղտնիությունը և դրանց անժխտելությունը: Տեղեկատվական անվտանգությունը նաև ներառում է այն միջոցները, որոնք անհրաժեշտ են սպառնալիքները հայտնաբերելու, նկարագրելու և սպառնալիքներին հակադարձելու համար:

Համակարգչային ցանցի գրոհներ

Համակարգչային ցանցի գրոհները բնութագրվում են որպես գործողություն, որոնք միտված են համակարգիչներում և այլ կրիչներում պահվող տեղեկատվության վնասմանը, հասանելիության խաթարմանը, ոչնչացմանը և գողացմանը: Համակարգչային ցանցի գրոհները իրականացվում են համակարգիչներով ընդդեմ համակարգիչների կամ համակարգչային ցանցերի:

Համակարգչային ցանցի գրոհների բնութագրիչներից է տվյալների արտահոսքը (Ventre 45):

Հարկ է տարբերակել էլեկտրոնային հարձակումը համակարգչայինից: Օրինակ՝ էլեկտրամագնիսական ուժի կիրառությունը և դրա միջոցով տեխնիկայի խափանումը համակարգչային գրոհ չէ, իսկ այլ համակարգիչ քարոզչական կամ այլ նպատակով նպատակով վիրուս մուտք անելը համակարգչային գրոհ է:

Այս հասկացությունը առնչվում է առավելապես կիբերանվտանգությանը, որը առանձին անդրադարձի թեմա է:

Վերը նշված սահմանումները և մոտեցումները տեղեկատվական պատերազմներին տրվող առավել տարածված և ընդհանրացված բնութագրումներն են: Միաժամանակ, ուսումնասիրելով ոլորտին առնչվող արևմտյան և ռուսական գիտական աղբյուրները, կարելի է նշել, որ արևմտյան տեսաբանները «տեղեկատվական պատերազմ» եզրույթը առավելապես ասոցացնում են տեղեկատվական տեխնոլոգիաների, ֆիզիկական տիրույթի հետ և հաճախ հանգում կիբերանվտանգությանը: Ռուսական աղբյուրներում տրվում է ավելի ընդհանրական սահմանում, սակայն շեշտը դրվում է քարոզչական-հոգեբանական բաղադրիչի վրա:

Որոշ մասնավոր դեպքերում տեղեկատվական պատերազմը ասոցացվում է տեղեկատվական պայքարի առավել կիրառելի և առավել ճանաչված ձևերից մեկի՝ քարոզչության հետ: Սակայն քարոզչությունը կարող է լինել տեղեկատվական քաղաքականության մի բաղադրիչը միայն, այնինչ տեղեկատվական պատերազմը լայն հասկացություն է, որը ենթադրում է ոչ միայն հոգեբանական ազդեցություն որևէ թիրախային խմբի վրա, այլ նաև ֆիզիկական-տեխնոլոգիական միջամտություն, սեփական տեղեկատվական տարածքի պաշտպանություն, տեխնիկական ապահովվածություն, ցանցային տիրույթի վերահսկողություն և այլն:

Տեղեկատվական օպերացիա

Տեղեկատվական պատերազմի երևույթի նկարագրության ժամանակ կիրառվում են հարակից այլ հասկացություններ ևս, որոնք տեղեկատվական պատերազմի առանձին բաղադրիչներ են: Դրանց շարքին է դասվում *տեղեկատվական օպերացիան*: Այն հաճախ թարգմանվում է որպես «տեղեկատվական գործողություն», սակայն մեր կարծիքով՝ հասկացության նման կիրառումը բավականին լայն բովանդակություն է ներառում, ըստ որի և՛ տեղեկատվական պատերազմը, և՛ գրոհը, և՛ դիմակայությունը, և առհասարակ ցանկացած գործընթաց կարելի է անվանել գործողություն: Հետևաբար, առավել նպատակահարմար է շրջանառել հենց «տեղեկատվական օպերացիա» եզրույթը:

Լայն իմաստով տեղեկատվական օպերացիաները այն գործողություններն են, որոնք ձեռնարկվում են ազդելու որոշումների կայացման վրա՝ ի պաշտպանություն սեփական քաղաքական և ռազմական նպատակների՝ ազդելով հակառակորդի տեղեկատվական գործընթացների և կառավարման համակարգերի վրա՝ միաժամանակ պաշտպանելով սեփական տեղեկատվական համակարգերը (R-techno Website): Տեղեկատվական գործողություններ իրականացնելիս լայնորեն կիրառվում են քարոզչական գործիքակազմեր: Ավելի նեղ իմաստով տեղեկատվական գործողությունները միտված են սեփական տեղեկատվական համակարգերը պաշտպանելուն, որի համար կիրառվում են հակառակորդի կողմից տեղեկատվության հավաքագրմանը, մշակմանը, փոխանցմանն ու պահպանմանը խոչընդոտող քայլեր:

ԱՄՆ տեղեկատվական օպերացիաների մշակմամբ ու համակարգմամբ զբաղվող գերատեսչական մոտեցումը տեղեկատվական օպերացիան սահմանում է որպես ԱՄՆ կառավարության կողմից իրականացվող պաշտոնական փորձ՝ մշակելու մի շարք դոկտրինալ մոտեցումներ՝ ի շահ սեփական ռազմական և դիվանագիտական ուժերի՝ օգտագործելով և գործարկելով տեղեկատվության ուժը: Տեղեկատվական օպերացիաների թիրախը հակառակորդի որոշում կայացնողներն են, ուստի ջանքերի մեծ մասը ուղղված են լինելու այդ անձին կամ մարդկանց խմբին որոշակի գործողություններ կատարել կամ չկատարել ստիպելուն (Armistead 25):

Մ. Չափլը և Դ. Սայդլը առանձնացնում են այսպես կոչված վարկաբեկող (offensive) և պաշտպանական (defensive) տեղեկատվական օպերացիաները: Հեղինակների մոտեցմամբ վարկաբեկող են այն տեղեկատվական օպերացիաները, որոնք ձեռնարկվում են հակառակորդի տեղեկատվությունը կամ տեղեկատվական գործողությունները մերժելու, շահարկելու, խափանելու կամ ոչնչացնելու համար: Պաշտպանական են այն տեղեկատվական օպերացիաները, որոնք ձեռնարկվում են սեփական տեղեկատվությունը կամ տեղեկատվական համակարգերը հակառակորդի ժխտման, շահարկման, խափանման կամ ոչնչացման փորձերից պաշտպանելու համար (Chapple, Seidl 15):

Դ. Կյուելը տեղեկատվական օպերացիաները սահմանում է որպես կառավարության և ռազմական ուժերի կողմից իրականացվող գործողություններ՝ կառավարելու և շահագործելու տեղեկատվական միջավայրը ազգային ուժի տեղեկատվական բաղադրիչի օգտագործման միջոցով (Kuehl 37):

Այս սահմանման մեջ տեղեկատվական օպերացիաների մենաշնորհը վերագրվում է պետությանն ու պետական կառույցին, այնինչ տեղեկատվական օպերացիան, ի տարբերություն տեղեկատվական պատերազմի կամ տեղեկատվական այլ տեսակի ակցիաների, կարող է իրականացվել ցանկացած, այդ թվում՝ անձնական մակարդակում:

Վ. Մակարովը տեղեկատվական օպերացիաները սահմանում է որպես տեղեկատվությանն առնչվող գործողություններ, որոնք ուղղված են գերակայության հասնելու տեղեկատվական՝ տեղեկատվական-կիբերնետիկ և տեղեկատվական-հոգեբանական տիրույթներում (Макаров 103):

Ինչպես երևում է՝ թե՛ դոկտրինալ, թե՛ գիտական ձևակերպումներում տեղեկատվական օպերացիաները ունեն և՛ տեխնիկական, և՛ հոգեբանական բաղադրիչ, որը շեշտվում է նաև Վ. Մակարովի ձևակերպման մեջ:

Հարկ է նշել, որ տեղեկատվական օպերացիաները ինչպես կարող են լինել տեղեկատվական պատերազմների բաղկացուցիչ մաս, այնպես էլ կարող են հանդես գալ որպես առանձին գործողություն: Վերջին դեպքում դրանք կարող են լինել կարճաժամկետ և նպատակին հասնելուց հետո չստանալ շարունակություն կամ կապակցված չլինել մեկ այլ տեղեկատվական գործողության հետ: Այս առումով տեղեկատվական օպերացիան լայն հասկացություն է և կարող է կիրառվել տարբեր համատեքստերում:

Տեղեկատվական օպերացիաները այնպիսի գործողություններ են, որոնք պետք է ունենան սահմանված ժամանակային սահմաններ և որոնց վերջնարդյունքը պետք է լինի հստակ չափելի: Այս հատկանիշները բնորոշ են նաև տեղեկատվական գրոհներին, սակայն եթե գրոհները հստակ հարձակողական գործողություններ են ենթադրում, տեղեկատվական գործողությունների դեպքում նման սահմանափակում չկա: Օրինակ՝ տեղեկատվական գործողության նպատակը կարող է լինել հակառակորդ կողմից որևէ ինֆորմացիայի ստացումը կամ սեփական երկրում սպասվող որևէ իրադարձության առիթով տրամադրությունների շոշափումը, որևէ գործողության համար հող նախապատրաստելը և այլն:

Տեղեկատվական դիմակայություն

Տեղեկատվական պատերազմների հաջորդ բաղադրիչը *տեղեկատվական դիմակայությունն* է: Մասնագիտական գրականությունում հաճախ «տեղեկատվական պատերազմ» և «տեղեկատվական դիմակայություն» եզրերը օգտագործվում են զուգահեռ՝ փոխարինելով մեկը մյուսին: Անգլիալեզու աղբյուրներում երկու տերմինների համար էլ կիրառվում է “Information Warfare” արտահայտությունը: Ռուսական աղբյուրներում տարանջատվում են “Информационная война” և “Информационное противоборство” տերմինները:

Լայն առումով այս երկու հասկացությունների՝ մեկը մյուսին փոխարինելը հասկանալի և ընդունելի է, քանի որ տեղեկատվական դիմակայությունը ևս սահմանվում է որպես «պետությունների կողմից տարվող պայքարի ձև և բաղկացուցիչ մաս, որում կողմերից յուրաքանչյուրը ձգտում է հակառակորդին վնասել տեղեկատվական միջոցներով» (Информационное Противоборство, www.encyclopedia.mil.ru, 31.10.2023):

Մեկ այլ սահմանման համաձայն այն «միջպետական հակամարտության ձև է, որը ենթադրում է հատուկ մշակված միջոցների օգտագործում՝ հակառակորդ կողմի տեղեկատվական ռեսուրսի վրա ազդելու և սեփական ռեսուրսները պաշտպանելու համար՝ ի շահ սեփական քաղաքական և ռազմական նպատակների» (Информационное противоборство на современном этапе: анализ и тенденции, “Молодой учёный”, N2):

Ինչպես տեսնում ենք, տեղեկատվական դիմակայության վերընշված բնութագրիչները գրեթե նույնական են տեղեկատվական պատերազմի բնութագրիչների հետ: Այնուամենայնիվ, այս երկու տերմինների միջև կա տարբերություն՝ կապված այն բանի հետ, թե տեղեկատվական պայքարում որ կողմն է պրոակտիվ: Տեղեկատվական դիմակայությունը ենթադրում է հակառակորդի կողմից արդեն իսկ ձեռնարկված տեղեկատվական գործողությունների, ընդհուպ տեղեկատվական պատերազմի հակադարձում: Այս առումով տեղեկատվական դիմակայությունը առավելապես ռեակտիվ գործողությունների շարք է, արդեն իսկ ձեռնարկված գործողություններին պատասխան արձագանքն է:

Այն դեպքում, երբ հակամարտող կողմերից որևէ մեկը աչքի չի ընկնում պրոակտիվ գործողություններով կամ մյուս կողմը առավելապես պաշտպանվողի

դիրքերում չէ, ևս ընդունելի է տեղեկատվական պատերազմին տալ «տեղեկատվական դիմակայություն» անվանումը:

Այս համատեքստում, տարընթերցումներից խուսափելու համար, տեղեկատվական գործողության ռեակտիվ տեսակը բնութագրելիս ավելի նախընտրելի է «տեղեկատվական դիմադրություն» եզրույթի կիրառումը, որն առավել հստակ է արտահայտում հասկացության իմաստային ծավալը: «Տեղեկատվական դիմադրության» դեպքում թե՛ անգլիալեզու, թե՛ ռուսալեզու աղբյուրներում հստակ սահմանվում է տեղեկատվական գործողության ռեակտիվ լինելը: Անգլիալեզու գրականության մեջ կիրառվում է “Information Resistance” կամ “Information Resilience” տերմինը, դե իսկ ռուսական աղբյուրներում այն հիշատակվում է որպես “информационное сопротивление”:

Հատկանշական է, որ ռուս-ուկրաինական պատերազմի ընթացքում ձևավորված համացանցային քարոզչական խմբերից մեկը ստացել է «Տեղեկատվական դիմադրություն» անվանումը: Այն ոչ կառավարական նախագիծ է, որի նպատակն է հակազդել Ուկրաինայի տեղեկատվական տարածքի նկատմամբ իրականացվող սպառնալիքներին, որոնք ուղղված են ռազմական, տնտեսական, էներգետիկ ոլորտներին, ինչպես նաև հենց բուն տեղեկատվական ոլորտին (Information Resistance, Euromaidan Press լրատվական ընկերության վեբ կայքը):

Ընդհանուր առմամբ, տեղեկատվական դիմադրությունը գործողությունների համալիր է, որն ուղղված է չեզոքացնելու հակառակորդ կողմից եկող տեղեկատվական գրոհները:

Այս գործում շատ կարևոր է ճիշտ գործիքակազմի ընտրությունը և ընտրված գործիքների ճիշտ կիրառումը: Տեղեկատվական դիմադրության բաղկացուցիչ մասն են՝

1. հակառակորդի կողմից առաջ քաշած թեզերին հակադարձումը՝ սեփական հակաթեզերի առաջ քաշմամբ և հիմնավորմամբ,
2. հակառակորդի կիրառած էլեկտրոնային պայքարի միջոցների չեզոքացումը,
3. սեփական կիբերտարածքի՝ հակառակորդի հնարավոր հարձակումներից պաշտպանումը,
4. միջազգային, ինչպես նաև տեղական մամուլում բարենպաստ տեղեկատվության տարածումը:

Այս ցանկը, իհարկե, շարունակելի է: Հարկ է ընդգծել տեղեկատվական դիմադրության միջոցների կիրառումից հետո սեփական գրոհների ձեռնարկումը: Վերջինս տեղեկատվական դիմադրության կարևորագույն և ամենից արդյունավետ բաղադրիչն է:

Իսկ տեղեկատվական դիմակայության, և առհասարակ տեղեկատվական պատերազմների ընթացքում ոչ խոցելի հասարակություն ունենալու համար կարևորվում են հետևյալ բաղադրիչները՝

- մեդիագրագիտություն (մեդիային, ստացվող տեղեկատվությանը քննադատաբար և գրագետ մոտեցում),
- տեղեկատվական հիգիենա (ստացվող տեղեկատվության մանրակրկիտ գնահատում՝ մինչ հավատալը կամ տարածելը),
- հանրային իրազեկում (սպասվող գործողությունների մասին հանրությանը իրազեկելը և դրանց ճիշտ արձագանքելուն պատրաստելը):

Այս ամենը հաճախ ենթադրում է երկարատև նախապատրաստություն և մեծ ջանքեր: Յուրաքանչյուր պետություն, որը գտնվում է տևական հակամարտության մեջ կամ նշմարում է հնարավոր սպառնալիքներ, պետք է համակարգված ջանքեր իրականացնի սեփական երկրում վերոնշյալ բաղադրիչների ուժեղացման ուղղությամբ:

Տեղեկատվական գրոհներ

Հաճախ տեղեկատվական գործողությունները սպասվող գործողությունների (ռազմական, դիվանագիտական) նախապատրաստական աշխատանքների հիմնական մասն են: Նման դեպքերում պետությունները հաճախ են իրականացնում այսպես կոչված *տեղեկատվական գրոհներ*: Տեղեկատվական գրոհները հաճախ էլ կարող են լինել իրականացվող պայքարի հիմնական գործիքը: Հատկապես ռազմական գործողությունները մշտապես ուղեկցվում են համապատասխան տեղեկատվական գրոհներով:

Տեղեկատվական գրոհները հետապնդում են մի քանի նպատակներ ՝

1. սպասվող գործողությունների համար հող նախապատրաստելը (այս կամ այն ձևով արդարացնելը սպասվող արարքները),
2. ստանալ հետադարձ (feedback) կապ սպասվելիք կամ մտածված գործողության վերաբերյալ,
3. ձեռնարկված գործողություններին տալ ցանկալի ընթացք,
4. մեղմել կատարված գործողության հետևանքների վերաբերյալ բացասական արձագանքը կամ վերացնել այն,
5. միջազգային հարաբերությունների այլ ակտորների առջև դրական կերպար ստեղծելը,
6. հակառակորդի վրա ճնշում կիրառելը,
7. հակառակորդի կողմից ձեռնարկվելիք գործողությունները բացասական լույսի տակ ներկայացնելը,
8. ինֆորմացիոն դաշտում հակառակորդի նկատմամբ առավելություն ունենալը:

Տեղեկատվական գրոհը սահմանվում է որպես պլանավորված, կազմակերպված և նպատակաուղղված զանգվածային գործողություն, որն ուղղված է հասցեատիրոջ վրա ազդելու միջոցով գրոհի կազմակերպիչների շահերին համապատասխան հասարակական կարծիքի ու վարքագծի ձևավորմանը:

Տեղեկատվական գրոհի իրականացման հիմնական գործիքները լրատվամիջոցներն ու համացանցն են (Дипломатический словарь առցանց բառարան):

Տեղեկատվական գրոհները, ի տարբերություն մշտական տեղեկատվական պատերազմի, ունենում են հստակ սահմանված ժամանակային սահմաններ (“Информационная атака: понятие и онтологические свойства”, Политическая лингвистика ամսագիր,
Раздель 2): Այս պնդումը տեղեկատվական օպերացիաների դեպքում ևս լիովին կիրառելի է:

Տեղեկատվական գրոհները ունենում են թիրախավորված լսարան կամ մարդկանց խումբ: Դրանց նպատակն է խաթարել հակառակորդի հեղինակությունը կամ ստանալ ցանկալի տեղեկատվության ավելի շատ լուսաբանում առավել ցանկալի ձևով: Հաճախ տեղեկատվական գրոհների ժամանակ թիրախային խմբին են ներկայացվում այնպիսի փաստեր կամ տեղեկատվություն, որը ստուգելը դժվար է կամ անհնար: Երբեմն տեղեկատվության նման հոսքը մատուցվում է բացառիկ լուրի տեսքով, ներկայացվում է որպես «բացահայտում», «գաղտնազերծում»: Ամեն ինչ արվում է գրգռելու համար թիրախային լսարանի հետաքրքրասիրությունը: Նմանատիպ դեպքերում, որպես կանոն, գտնվում է թիրախային լսարանին հետաքրքիր որևէ լրահոս, այնուհետև որոշվում է տարածման աղբյուրը: Տեղեկատվական գրոհների հաջողությունը մեծապես պայմանավորված է դրանց կիրառման հետևողականությամբ, թիրախային լսարանի մշտադիտարկմամբ, թեման ըստ անհրաժեշտության «թեժ» պահելու մարտավարությամբ, ինչպես նաև հակառակորդի հնարավոր պատասխան գործողությունների կանխատեսմամբ:

Տեղեկատվական գրոհի արդյունավետությունը նկատելի է դառնում նրա ավարտից հետո և գնահատվում է *որակական* ու *քանակական* չափանիշներով:

Որպես քանակական չափանիշ կարելի է դիտարկել այն լսարանի կամ թիրախային խմբի մեծությունը, որի վրա տվյալ տեղեկատվական գրոհը այս կամ այն չափով ունեցել է ազդեցություն: Իսկ որպես որակական ցուցիչ դիտարկվում է հենց վերջնարդյունքը. արդյոք ձեռնարկված տեղեկատվական գրոհը տվել է ցանկալի արդյունքը թե ոչ: Օրինակ՝ եթե տեղեկատվական գրոհի նպատակը որևէ զանգվածի ուղղորդելն է քվեարկել այս կամ այն անձի կամ որոշման օգտին, և արդյունքում հաջողվում է ստանալ մեծամասնության քվեն կամ համակրանքը, ապա տեղեկատվական գրոհը կարելի է համարել հաջողված:

Տեղեկատվական գրոհները կարող են լինել ուղղակի և անուղղակի:

Ուղղակի տեղեկատվական գրոհը բաղկացած է հակառակորդի տեղեկատվական տարածք անմիջական ներխուժումից և նրա միջավայրում կեղծ տեղեկատվության ներմուծումից: *Անուղղակի* տեղեկատվական գրոհը կարող է դրսևորվել ոչ հավաստի կամ ոչ ճիշտ տեղեկատվության ստեղծմամբ, որը հակառակորդին հրամցվում է որպես ճշմարտություն: Երկրորդ դեպքում հակառակորդի տեղեկատվական դաշտում ներքին միջամտություն տեղի չի ունենում (Дипломатический словарь առցանց բառարան):

Ինչպես վերընշվածից երևում է, տեղեկատվական գրոհը ինֆորմացիոն հոսքերի միջոցով իրականացվող գործողություն է: Այն դասվում է տեղեկատվական-հոգեբանական պատերազմի մեթոդների թվին: Սակայն արևմտյան աղբյուրներում «տեղեկատվական գրոհ» հասկացությունը առավելապես ասոցացվում է կիբեր գրոհների հետ և ֆիզիկական ներխուժում է՝ գրոհ հակառակորդի համակարգիչների, հաշվողական համակարգերի, համակարգչային ցանցի վրա՝ չարտոնված մուտք ստանալու նպատակով և վնաս պատճառելու մտադրությամբ: Կիբերհարձակումները նպատակ ունեն անջատելու, խափանելու, ոչնչացնելու կամ վերահսկելու համակարգչային ցանցերը կամ փոխելու, արգելափակելու, ջնջելու, շահարկելու կամ գողանալու այդ համակարգերում պահվող տվյալները (Pratt, TeckTarget տեխնոլոգիական կայք):

ԱՄՆ Ստանդարտների և տեխնոլոգիաների ազգային ինստիտուտի սահմանման համաձայն՝ տեղեկատվական օպերացիաները (հարձակվողական) այնպիսի գործողություններն են, որոնք փորձում են հավաքել, խաթարել, հերքել, նսեմացնել կամ ոչնչացնել տեղեկատվական համակարգի ռեսուրսները կամ բուն տեղեկատվական համակարգը: Մեկ այլ ձևակերպմամբ՝ դրանք հարձակումներ են կիբերտարածության միջոցով, որոնք թիրախավորում են ձեռնարկության կողմից կիբերտարածության օգտագործումը՝ նպատակ ունենալով խափանել, անջատել, ոչնչացնել կամ վերահսկել համակարգչային տիրույթը, կամ էլ ոչնչացնել տվյալների ամբողջականությունը կամ գողանալ վերահսկվող տեղեկատվությունը (Website of National Institute of Standards and Technologies):

Վերջին ձևակերպումը կրկնում է Ք. Պրատի տված կիբերհարձակման սահմանումը:

Կիբերհարձակումները տարբերվում են տեղեկատվական գրոհներից, տեղեկատվական պատերազմների առանձին բաղադրիչ են և առանձին ուսումնասիրության նյութ:

Այն հիմնական հատկանիշներ, որոնցով տեղեկատվական գրոհները ձեռք են բերում առանձնահատուկ բնույթ և առանձնանում են տեղեկատվական պատերազմների մյուս բաղադրիչներից, հետևյալներն են՝ անկանխատեսելիություն, պրոակտիվություն, արագություն, թիրախայնություն և արդյունքների հստակ չափելիություն:

Եզրահանգումներ

Ամփոփելով հոդվածը՝ կարելի է արձանագրել, որ աշխարհի տարբեր մասերում տեղի ունեցող տարաբնույթ հակամարտությունները ուղեկցվում են տեղեկատվական պատերազմների տարբեր բաղադրիչներով: Ի հավելումն սրա՝ կարող ենք անել հետևյալ եզրահանգումները.

- Միջազգային խոշոր շատ դերակատարներ մինչ տնտեսական, ռազմական կամ քաղաքական ոլորտում որևէ խոշոր նախաձեռնություն իրականացնելը դիմում են լավ մշակված տեղեկատվական գործողությունների: Հաճախ տեղեկատվական պատերազմը «տաք» պատերազմի նախերգանքն է, երբեմն էլ «տաք» պատերազմին փոխարինելու է գալիս տեղեկատվական պատերազմը: Տեղեկատվական պատերազմի նախապատրաստումը կամ դրա անմիջական վարումը կարող է տևել տարիներ, անգամ տասնամյակներ:
- Այս ոլորտի առաջատար շատ պետություններ, օգտագործելով տեղեկատվական պատերազմի տարբեր բաղադրիչներն ու գործիքակազմերը, կարողանում են տեղեկատվական գերակայության հասնել իրենց հիմնական հակառակորդների նկատմամբ՝ միաժամանակ բարենպաստ հանրային կարծիք ստեղծելով իրենց արտաքին քաղաքական շահերն առաջ տանելու համար: Այս ոլորտում կարելի է առանձնացնել ԱՄՆ-ի վարած «փափուկ ուժի» քաղաքականությունը:

Քննարկման տեղիք չի տալիս այն փաստը, որ ցանկացած պետություն իր քաղաքականությունը իրականացնում է սեփական շահերից դրդված: Եթե գիտության տեսանկյունից լավ կամ վատ, դրական կամ բացասական պետությունների տարանջատումը հակագիտական կարող է հնչել, ապա մարդկանց ընկալումներում այն այլ է, և այդ ընկալումների վրա մեծապես ազդում է պետությունների իրականացրած տեղեկատվական քաղաքականությունը:

Յուրաքանչյուր պետության առջև դրված խնդիրներից է օգտագործել տեղեկատվական պայքարի ընձեռած գործիքակազմերը՝ նպաստավոր դիրք, համբավ ձեռք բերելու, հակառակորդի նկատմամբ առավելություն ունենալու և լայն շրջանակների համակրանքը շահելու համար:

Գտնվելով հակամարտությունների գոտում և ունենալով սահմանափակ նյութական ռեսուրսներ, թե՛ իմիջի ձևավորման, թե՛ սեփական թեզերը առաջ տանելու և լսելի դառնալու, թե՛ հակառակորդի կեղծ թեզերին ու տեղեկատվական գրոհներին դիմակայելու համար՝ մեր երկրին անհրաժեշտ է ճիշտ տեղեկատվական քաղաքականության մշակում և իրականացում: Հոդվածում դիտարկվող տեղեկատվական գործողությունների կազմակերպումը և պետական մակարդակով իրականացումը պահանջում են լուրջ և համակարգված ջանքեր և որ ամենակարևորն է՝ հետևողականություն:

ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅՈՒՆ

1. ՀՀ *Ազգային անվտանգության ռազմավարություն*, *Բաց և անվտանգ տեղեկատվական և կիբերտիրույթների ապահովում*, Երևան, 2020, https://www.primeminister.am/u_files/file/Different/AA-Razmavarutyun-Final.pdf: Վերջին մուտք՝ 18.11.2023թ.:

2. Armistead, Leigh. *Information Operations. Warfare and the Hard Reality of Soft Power.* Joint Forces Staff College and the National Security Agency, 2004.

3. Chapple, Mike; Seidl, David. *Cyberwarfare: Information Operations in a Connected World.* Burlington, 2015.

4. Hutchinson, William; Warren Matthew. *Information Warfare: Corporate Attack and Defence in a Digital World*. London, 2001.

5. “Information Resistance”, *“Euromaidan Press” Information Company Website*. https://euromaidanpress.com/author/informationresistance/. Accessed: 05.11.2023թ.:

6. Kuehl, Daniel. *Information Operations, Information Warfare, and Computer Network Attack. Their Relationship to National Security in the Information Age.* International Law Studies, Volume 76. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1400&context=ils. Accessed: 29.10. 2023.

7. "Cyber Attack". *National Institute of Standards and Technologies Website*, https://csrc.nist.gov/glossary/term/cyber_attack. Accessed: 22.11.2023.

8. "Media – (Dis)information – Security". *NATO website,* https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf. Accessed: 19.11.2023.

9. Pratt, Mary K. Cyber Attack, "Cyber Attack", *TeckTarget Technological Website*. https://www.techtarget.com/searchsecurity/definition/cyber-attack. Accessed: 19.11.2023.

10. US Department of Air Force. *Information Warfare*. 1996, https://www.google.am/books/edition/Information_Warfare/kK0ChVZRL5QC?hl=en&gbpv=1&dq=information+warfare&printsec=frontcover. Accessed: 17.11.2023.

11. Ventre, Daniel. *Information Warfare*. London, 2016, 2nd edition.

12. «Информационная атака», Дипломатический словарь, http://diplomaticdictionary.com/dictionary/информационная-атака/. Доступно: 05.11.2023.

13. Коцюбинская, Любовь Вячеславовна, «Информационная атака: понятие и онтологические свойства», *Политическая лингвистика журнал*. Раздел 2, Москва, https://cyberleninka.ru/article/n/informatsionnaya-ataka-ponyatie-i-ontologicheskie-svoystva/viewer. Доступно: 05.11.2023.

14. Иванцов, Алексей Васильевич, «Информационные войны в современном мире: понятие, сущность и содержание», https://elib.bsu.by/bitstream/123456789/286723/1/24-35.pdf. Доступно 30.08.2024.

15. «Информационные операции - что это такое?», *R-techno website*, https://r-techno.com/ru/Information-operations/. Доступно: 31.10.2023.

16. «Информационное противоборство». www.encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221. Доступно: 31.10.2023.

17. «Информационное противоборство на современном этапе: анализ и тенденции». *Молодой учёный*, N2, Москва, 2009, https://moluch.ru/archive/2/153/. Доступно: 31.10.2023.

18. Макаров, Василий Емельянович. *Политические и социальные аспекты информационной безопасности*. Москва, 2015.

19. Панарин, Игорь. *Первая мировая информационная война: развал СССР*. Москва, 2010.

WORKS CITED

1. HH Azgayin anvtangut'yan r'azmavarut'yun, Bac ev anvtang teghekatvakan ev kibertiruyt'neri apahovum [RA National Security Strategy, Ensuring Open and Secure Information and Cyberspace], Erevan, 2020, https://www.primeminister.am/u_files/file/Different/AA-Razmavarutyun-Final.pdf. verjin mutqy'` 18.11.2023t'. (in Armenian)

2. Informacionnaja ataka, Diplomaticheskij slovar'. [Information Attack]. http://diplomaticdictionary.com/dictionary/informacionnaja-ataka/. Poslednij vhod: 05.11.2023. (in Russian)

3. “Informacionnaja ataka: ponjatie i ontologicheskie svojstva”, Politicheskaja lingvistika zhurnal. Razdel' 2, Moskva, Kocjubinskaja, Ljubov Vjacheslavovna, [Information Attack: Concept and Ontological Properties]. https://cyberleninka.ru/article/n/informatsionnaya-ataka-ponyatie-i-ontologicheskie-svoystva/viewer Poslednij vhod: 05.11.2023. (in Russian)

4. Informacionnye voyni v sovremennom mire: pojatije, sushnost I soderzhanie, Ivantsov, Aleksei Vaslievich, [Information Warfare: Concept, Essence and Content], https://elib.bsu.by/bitstream/123456789/286723/1/24-35.pdf. Poslednij vhod: 30.08.2024. (in Russian)

5. Informacionnye operacii - chto jeto takoe?, R-techno web site. [What is information operation?]. https://r-techno.com/ru/Information-operations/. Poslednij vhod: 31.10.2023.

6. Informacionnoe Protivoborstvo. [Information Resistance]. www.encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221. Poslednij vhod: 31.10.2023. (in Russian)

7. Informacionnoe protivoborstvo na sovremennom jetape: analiz i tendencii. “Molodoj uchjonyj”, N2, Moskva, 2009, [Information Resistance in Modern Stage: Analysis and Trends]. https://moluch.ru/archive/2/153/. Poslednij vhod: 31.10.2023. (in Russian)

8. Makarov, Vasilij Emel'janovich. Politicheskie i social'nye aspekty informacionnoj bezopasnosti. Moskva 2015. (in Russian)

9. Panarin, Igor'. Pervaja mirovaja informacionnaja vojna: Razval SSSR. [First Information World War: Collapse of USSR]. Moskva, 2010. (in Russian)

ON THE CONCEPT OF INFORMATION WARFARE

ANNA SISOYAN
Yerevan State University,
Department of International Relations,
Chair of Political Science, Ph.D. Student
Yerevan, the Republic of Armenia

The purpose of the article is to study the concept of "Information Warfare" and its components. In particular, the concepts of information warfare, information operation, information confrontation and information attack are separately discussed, the substantive and semantic relations of above-mentioned components are revealed. n order to achieve the goal, we set ourselves the following tasks: to study the approaches and definitions of the concepts mentioned in Western and Russian sources, to make a comparison and to highlight the prerequisites for the effective use of the components of information warfare.

Descriptive, comparative and analysis methods were used during the research.

Formulations and approaches put forward by well-known theoreticians and specialists of the field were used as a source in the article.

Within the framework of the article, the modern tools for conducting competent information wars in the context of the implementation of the foreign policy of the states are also considered.

In the result of the research it was concluded that the competent use of various components and tools of information war gives an opportunity to achieve superiority over the enemy. In order to resist the enemy's fake theses and information attacks, our country needs the development and implementation of the correct information policy, which in turn requires serious and coordinated efforts and consistency at the state level.

Key words: *Information Warfare, Information Resistance, Information Operation, Cyberspace, Cyber Attacks.*

К ВОПРОСУ О ПОНЯТИИ ИНФОРМАЦИОННОЙ ВОЙНЫ

АННА СИСОЯН
соискатель кафедры политологии
факультета международных отношений
Ереванского государственного университета,
г. Ереван, Республика Армения

Цель статьи – исследование понятия «Информационная война» и ее компонентов. В частности, отдельно рассматриваются понятия информационной войны, информационной операции, информационного противоборства и информационной атаки, раскрываются содержательные и смысловые связи названных компонентов. Для достижения цели мы поставили перед собой следующие задачи: изучить подходы и определения понятий, упомянутых в западных и российских источниках, провести сравнение и выделить предпосылки эффективного использования компонентов информационной войны.

В ходе исследования использовались описательный, сравнительный и аналитический методы.

В качестве источников в статье использованы формулировки и подходы, выдвинутые известными теоретиками и специалистами данной области.

В рамках статьи также рассматриваются современные инструменты ведения грамотных информационных войн в контексте реализации внешней политики государств.

В работе мы пришли к выводу о том, что грамотное использование различных компонентов и инструментов информационной войны дает возможность добиться превосходства над противником. Чтобы противостоять фейковым тезисам и информационным атакам противника, нашему государству необходима разработка и реализация правильной информационной политики, что, в свою очередь, требует серьезных и скоординированных усилий и последовательности на государственном уровне.

Ключевые слова: *информационная война, информационное противостояние, информационная операция, киберпространство, кибератаки.*