ԱՆՏԵՍԱՆԵԼԻ ԿԻԲԵՌՊԱՏԵՐԱԶՄԸ

Յանոս Խարալամբիդիս[*]

Ներածություն

Միջազգային համակարգում դեռևս գերակայում են ինքնիշխան ազգային պետությունները, որոնք հանդես են գալիս որպես գլոբալ համակարգի հիմնական կառուցվածքային դերակատարներ: Այնուհանդերձ, ազգային պետությունները գլոբալ հարթակում գործունեություն ծավալած միակ դերակատարները չեն: Շուկաները և վերազգային հսկաները, նույնիսկ այնպիսի ահաբեկչական կազմակերպությունները, ինչպիսին «Ալ Քաիդան» է, նույնպես գործում են գլոբալ ասպարեզում (*Charalambides,* 2013, pp.71-77; *Katzman,* 2005, pp.4-5, 7-8; *Bjelopera,* 2011, pp. 36-37)՝ նպատակ հետապնդելով փոփոխության ենթարկել միջազգային համակարգի կառուցվածքը: Այս առումով նշված միջազգային դերակատարները ձգտում են փոխարինել միջազգային ասպարեզում գերիշխող պետություններին (*Charalambides,* 2013, pp. 71-75, 45-52): Իշխանության բաղադրիչներից մեկը տեխնոլոգիան է, և հետևապես հարկ է ուսումնասիրել այն դերը, որ ունի տեխնոլոգիան միջազգային համակարգում՝ գերիշխանության շուրջ ընթացող «խաղերում» (*Charalambides,* 2010, pp. 34-35; *Ifestos and Platias,* 1992, pp. 83-84; *Morgenthau,* 1978, pp. 9-14; *Dougherty and Pfaltzgraff,* 1992, p. 115):

Հոդվածում քննարկվում է տեխնոլոգիայի կարևորությունը ներկա դարաշրջանում, մասնավորապես նոր տիպի պատերազմի, այն

[*] Միջազգային հարաբերությունների և եվրոպագիտության դոկտոր, Կիպրոս:

է՝ կիբեռպատերազմի համատեքստում: Այս կարգի պատերազմը համապատասխանում է միջազգային համակարգում տեղի ունեցող կառուցվածքային փոփոխություններին, որտեղ տեխնոլոգիան խաղում է իր ուրույն, նշանակալի դերը (*Charalambides*, 2013, pp. 12-13):

Սույն վերլուծությունում շոշափվում են այնպիսի հարցեր, ինչպիսիք են տարբեր տիպի պատերազմները, կիբեռպատերազմին սահմանում տալու և դրա գործնական իրականացումը բացատրելու փորձերը: Այս նկատառումով քննարկվում են միջազգային համակարգի զարգացման վրա կիբեռպատերազմի թողած ազդեցությունը և դրա արդյունքում տեղի ունեցող կառուցվածքային փոփոխությունները, ինչպես նաև այն կարևոր դերը, որ միջազգային ասպարեզում ունեն կիբեռպատերազմը և տեխնոլոգիան: Բարձրացվել է տեղին մի հարց, որի պատասխանը մենք պետք է գտնենք. հաղթական արդյունքի հասնելու համար բավարա՞ր են արդյոք հզորության այնպիսի դասական բաղադրիչները, ինչպիսիք են ռազմական ուժը, տարածքն ու բնակչության մեծությունը, բանակի մարտական ոգին և հմուտ ղեկավարությունը, թե՞ տեխնոլոգիան ինքնին կամ այլ միջոցների համակցությամբ կարող է շեշտակի փոփոխություններ բերել պատերազմների և միջազգային համակարգի կառուցվածքում (*Charalambides,* 2010, *Dougherty and Pfaltzgraff*, 1992, p. 168; *Gilpin*, 1981): Առ այսօր մեծ տերություններն անպարտելի են թվում: Այնուհանդերձ, երկու հարցեր պատասխանի կարիք ունեն. ճի՞շտ է արդյոք այդ հիպոթեզը և կարո՞ղ է արդյոք տեխնոլոգիան Գողիաթին հաղթած Դավիթի հինավուրց առասպելը կյանքի կոչելու հնարավորություններ ստեղծել:

1. Պատերազմի տարբեր տեսակները

Ներկա ժամանակաշրջանում միջազգային համակարգում տեղի են ունենում տարբեր տեսակի պատերազմներ:

Նախ՝ դրանք դասական պատերազմներն են, որոնցում ներգրավված կողմերը կիրառում են սովորական կամ նույնիսկ միջուկային զինատեսակներ: Դրանք այն պատերազմներն են, որ բռնկվում են երկու կամ ավելի պետությունների միջև: Քաղաքացիական կամ կրոնական պատերազմները, օրինակ՝ ներկայումս Սիրիայում ընթացողը (*CNN News,* 2012; *CNN News,* 2012a; *CNN News,* 2012b), ընդգրկում են այս դասական պատերազմների կարգում: Սովորաբար պետությունների կառուցվածքներում դրանք հանգեցնում են այնպիսի փոփոխությունների, որոնք տարածաշրջանային կամ գլոբալ մակարդակով անդրադառնում են միջազգային հարաբերությունների վրա: Եգիպտոսի օրինակով կարելի է դիտարկել կառուցվածքային փոփոխությունների հանգեցրած խոռվությունների հետևանքները: Թեպետ Մուբարաքի վարչակարգը կառուցված էր թերի ժողովրդավարության հիման վրա, այն կայունացնող գործոն էր դարձել տարածաշրջանային և գլոբալ համակարգերում: Մուբարաքի վարչակարգը ջանք չէր խնայում կայունացման ապահովման և հարևան Իսրայելի հետ խաղաղության պահպանման համար: Վարչակարգի տապալումից հետո Իսրայելի հետ սահմանին լարվածության օջախներ առաջացան (*CNN,* 2011, *Charalambides,* 2012, p. 6): «Մուսուլման եղբայրների» առաջնորդ Մուհամեդ Մուրսին 2012թ. հունիսի 24-ին պաշտոնապես հաղթող ճանաչվեց Եգիպտոսի առաջին ազատ նախագահական ընտրություններում՝ փոքր առավելության հասնելով Ահմեդ Շաֆիքի հանդեպ: Մուրսին հավաքել էր ձայների 51,7%-ը, իսկ Շաֆիքը՝ 48,2%-ը (*CNN News,* 2012c; *BBC News,* 2012): Քաղաքական իրավիճակը երկրում անկայուն է, և Եգիպտոսի նոր քաղաքական համակարգում «Մուսուլման եղբայրների» խաղացած քաղաքական, սոցիալական և ինստիտուցիոնալ դերը դարձել է ԱՄՆ-ի ու Իսրայելի մտահոգության առարկան: Հարցն այն է, թե արդյոք Եգիպտոսի ժողովրդի ապստամբությունը կբերի ժողովրդավարական քաղաքական համակարգի ստեղծման, թե

«Մուսուլման եղբայրները» կփորձեն քաղաքական համակարգը կենտրոնացնել իրենց ձեռքում՝ այն կառավարելիս առաջնորդվելով իսլամական օրենքներով: Եգիպտոսը տառապում է քաղաքական անկայունությունից և գտնվում է քաղաքացիական ու կրոնական պատերազմի եզրին: Հետևապես, Եգիպտոսում ստեղծված իրավիճակը կառուցվածքային փոփոխություններ առաջացրեց պետությունում և անդրադարձավ տարածաշրջանային համակարգի կայունության վրա:

Երկրորդ՝ ահաբեկչության դեմ պայքարը յուրօրինակ պատերազմ է պետությունների և ահաբեկչական կազմակերպությունների միջև, որոնցից է, օրինակ, միջազգային համակարգի ներկայիս կառուցվածքը փոփոխության ենթարկելու նպատակ հետապնդող «Ալ Քաիդան» (*Bin Laden,* 2005; *Almasmari, Jamjoom and Abedine,* 2012): Միաժամանակ, մենք վկա ենք դարձել անդադար մի պայքարի, որն ընթանում է երկու տեսակի գլոբալացումների միջև՝ արևմտյան և իսլամական: Վերջինս, անշուշտ, նպատակաուղղված է գլոբալ խալիֆաթի հիմնմանը (*Elsea,* 2007, pp. 10-15; *Lecker,* 2008, pp. 251-253): Նշված հակամարտությունը երբեմն ընդունում է նաև կրոնական պատերազմի ձև:

Երրորդ՝ պետությունների և շուկաների միջև պատերազմը հանգեցրեց ներկայիս տնտեսական ճգնաժամին: Անտեսանելի լինելով հանդերձ՝ շուկաները փորձում են գերիշխող դեր ունենալ միջազգային համակարգում: Հետևաբար, տեղին է հարցադրել. ի՞նչ է շուկան: Այս հարցին պատասխանող կարճ սահմանումը հետևյալն է. շուկան իրավատնտեսական գործընթաց է, որի միջոցով պահանջարկն ու առաջարկը համադրվում են՝ կանխորոշելով և սահմանելով շուկայական գները: Շուկան գործոնների և միջազգային համակարգում գործող դերակատարների վերացական կազմ չէ: Հակառակը՝ այն միջազգային համակարգում գործող կենսունակ կազմակերպություն է, որը բաղկացած է հետևյալ միավորներից.

1. Բոլոր տեսակի ընկերությունները (փոքր, միջին, մեծ) և առևտրատնտեսական կամ ֆինանսական գործունեություն իրականացնող այլ կազմակերպությունները, ինչպես նաև ընկերություններն ու տնտեսության ճյուղերը կառավարող անձինք, որոնց թվին են պատկանում սեփականատերերը, բաժնետերերը, կառավարիչները և տնօրենները։
2. Արտադրողական ուժերը, որոնք կազմված են արտադրության և աշխատանքի միջոցների համակցությունից (գործիքներ, հող և ենթակառուցվածքներ), ինչպես նաև մարդկային աշխատուժից (*Marx,* 1955)։
3. Կապիտալը և փողը ձեռնարկատերերի կողմից կիրառվող գործիքներ են՝ շահույթ, հարստություն և աճ ստեղծելու նպատակով։ Սակայն դրանք նաև օգտագործվում են աշխատողների (քաղաքացիական անձանց) կողմից՝ որպես եկամուտ (աշխատավարձ, շահատոկոսային եկամուտ, դիվիդենդ և այլն)՝ իրենց սպառողական պահանջմունքները բավարարելու նպատակով։
4. Բանկային համակարգը՝ ազգային, մասնավոր և միջազգային բանկային հաստատությունները և բանկիրները, որոնք վճռորոշ դերակատարում ունեն տեղական և գլոբալ ֆինանսական գործունեությունում։
5. Ֆոնդային բորսաները և արժեթղթային գործարքներ իրականացնող բրոքերները։
6. Քաղաքական և տնտեսական գործունեությունը կարգավորող միջազգային կազմակերպությունները, բանկերը և հզոր պետությունների խմբերը, ինչպիսիք են Մեծ քսանյակը, Արժույթի միջազգային հիմնադրամը, Վերակառուցման և զարգացման համաշխարհային բանկը, ինչպես նաև Առևտրի համաշխարհային կազմակերպությունը։

7. Բոլոր այն անձինք, ովքեր ուղղակիորեն կամ անուղղակիորեն ներգրավված են շուկաներում, այդ թվում՝ իրավաբանները, բանկիրները, հաշվապահները, քաղաքական գործիչները, աշխատողները (աշխատուժը) և սպառողները, արհմիություններն ու դրանց անդամները, քաղաքական կուսակցությունները, նախարարները և կառավարությունները: Հաճախ կուսակցությունները, քաղաքական գործիչները և կառավարությունները ֆինանսավորում են ստանում բիզնեսի աշխարհից կամ քաղաքացիներից, ավելի կոնկրետ՝ բանկիրներից, գործարարներից և շարքային քաղաքացիներից:
8. Էներգիայի մատակարարները և էներգամատակարարման շղթայում ընդգրկված բոլոր գործոնները: Ավանդական և վերականգնվող աղբյուրներից էներգիայի մատակարարման մեջ ներգրավված են թե՛ պետությունները, թե՛ անհատները, իսկ ինժեներ–մասնագետների և սարքավորումների միջոցով ապահովվում է էներգիայի առաքումը վերջնական սպառողներին (արդյունաբերական օբյեկտներ, բնակարաններ), ընդ որում, միջնորդները որոշում են էներգետիկ սակագները:
9. Հետազոտական կենտրոնները, համալսարանները և նորարարություն ստեղծող այլ տիպի հաստատությունները, որոնք ձևավորում են նոր ապրանքներ կամ դրանց զարգացման, հետևապես՝ որակի բարելավման նոր ուղիներ:
10. Կենտրոնական կառավարությունները, որոնք պետական ապարատի համատեքստում պարտավոր են անվտանգություն և կայունություն ապահովել տնտեսական և այլ գործունեություն ծավալող բոլոր միավորների համար:
11. Միջազգային և տեղական ֆինանսական և առևտրային օրենսդրությունը և այլ կարգավորողները, որոնց միջոցով կարելի է չափել ու գնահատել կանոնների, օրենքների, հանձնարարա-

կանների և ընդունված կարգերի իրական կատարման մակարդակների համապատասխանությունը:

12. «Վարկանիշային գործակալությունները», որոնց իրավունք է վերապահված գնահատել և այդպիսով բարձրացնել կամ իջեցնել մասնավոր բանկերի և ընդհանրապես՝ բանկային ոլորտի վարկանիշները: Փաստորեն, նրանք վճռորոշ դերակատարում ունեն գլոբալ ֆինանսական և քաղաքական համակարգում (օր.՝ *Standard & Poor's, Moody's and Fitch* վարկանիշները): «Վարկանիշային գործակալություններն» օգտագործվում են ներդրողների, արժեթղթեր թողարկողների, ներդրումային բանկերի, բրոքերների, կառավարությունների կողմից ապահովության նպատակով, իրենց ֆինանսական շահերը պաշտպանելու և ֆինանսական ռիսկը նվազեցնելու համար: «Վարկանիշային գործակալությունները» կազմում են հաշվետվություններ, որոնցում վարկային ռիսկը վերլուծվում է՝ նպատակ հետապնդելով պաշտպանել ներդրողներին և բարձրացնել շուկայի արդյունավետությունը: Ներկայիս տնտեսական ճգնաժամի պատճառով ԱՄՆ-ը և ԵՄ-ը (այդ թվում՝ ԵՄ անդամ երկրները) հարցականի տակ են դնում «վարկանիշային գործակալությունների» վստահելիությունը: Շուկաները գործուն կազմակերպություններ են, որտեղ մարդիկ խաղում, աշխատում, գործում ու փոխազդում են, և այդպիսով հոգեբանությունը մշտապես վերածվում է քաղաքական և տնտեսական գործիքի, որը կարող է օգտագործվել «վարկանիշային գործակալությունների» կողմից՝ «կասկածելի շահերի» օգտին շուկաների վրա ազդեցություն գործելու նպատակով: Հաշվետվությունների պատրաստման ժամանակը և ձևը հաճախ ձևավորում են պետության տնտեսական և քաղաքական իրավիճակը, դրա բանկային ոլորտը, ֆինանսական կարգավիճակը և պետական պարտքը, բացասական կամ դրական ազդեցություն են թողնում խնդրո առարկա

հանդիսացող պետության շուկայի և տնտեսության վրա, ինչպես նաև ընդհանուր առմամբ՝ բոլոր շուկաների վրա։

13. Արժույթի արժեքը և փոխարժեքները շուկայի վճռորոշ գործիքներ են՝ ֆինանսական գործարքների համար։

2. Կիբեռպատերազմի սահմանումը

Պատերազմների վերը նշված տեսակներից բացի, արժանահիշատակ է ևս մեկը։ Դա տեխնոլոգիական զարգացմանը բնորոշ կիբեռպատերազմն է, որը մշտապես կիրառվում է բազմատեսակ այլ պատերազմների համատեքստում։ Նման պատերազմում ներգրավված կողմերը կիրառում են բարձր տեխնոլոգիաներ։ Կիբեռպատերազմն ավելի ծավալուն էլեկտրոնային պատերազմի մաս է կազմում, դրա ընթացքում տեխնոլոգիական միջոցները շահագործվում են որպես անփոխարինելի գործիքներ՝ դասական, ավանդական կամ որևէ այլ տիպի հակամարտությունում հաղթանակի հասնելու համար։ Փորձելով սահմանում տալ կիբեռպատերազմին՝ ԱՄՆ պետական անվտանգության փորձագետ Ռիչարդ Ա. Կլարկը նշում է. *«Երբ այս գրքում օգտագործում ենք «կիբեռպատերազմ» եզրույթը, նկատի ունենք մեկ ազգային պետության կողմից մեկ այլ պետության համակարգիչներ կամ ցանցեր ներթափանցելու փորձերը՝ նպատակ հետապնդելով վնաս հասցնել կամ խաթարումներ առաջացնել»* (*Clarke,* 2010, p. 6)։

Բացի այդ, *Economist* հանդեսում կիբեռպատերազմը բնորոշվում է որպես *«պատերազմական գործողությունների հինգերորդ թատերաբեմ» (ի հավելումն ցամաքում, ծովում, օդային տարածքում և տիեզերքում իրականացվող գործողությունների)* (*Economist,* 2010), իսկ ԱՄՆ պաշտպանության փոխքարտուղար Վիլյամ Ջ. Լինը ընդգծում է, որ *«որպես դոկտրինային հարց, Պենտագոնը պաշտոնապես ճանաչել է կիբեռպատերազմն իբրև պատերազմի նոր ոլորտ... որը նույնքան կարևոր է դարձել, որքան ցամաքում, ծովում, օդում և*

տիեզերքում իրականացվող ռազմական գործողությունները» (Lynn, 2010, p. 97-98)։

Կան կիբեռպատերազմի մի քանի այլ կարճ սահմանումներ։ Սակայն կարելի է փաստել, որ կիբեռպատերազմը հնարավոր չէ ճշգրտորեն սահմանել։ Եվրոպական խորհրդարանի անվտանգության և պաշտպանության ենթահանձնաժողովի պատվիրած հետազոտությունում նշվում է. *«Կիբեռպատերազմի ընդհանուր սահմանում գոյություն չունի։ Էստոնիայի վրա կատարված հարձակումները 2007թ., Վրաստանի վրա՝ 2008թ., Stuxet-ի տարածումը կամ բարձր մակարդակի կիբեռլրտեսությունը, այս ամենը ժամանակին կոչվել են կիբեռպատերազմ։ Նույնիսկ պետությունների միջև հակամարտությունների հետ ամենայն հավանականությամբ առնչություն չունեցող կիբեռհարձակումները, օրինակ՝ «հակտիվիզմը», կամ 2010թ. «Վիքիլիքս»-ի հետ կապված իրադարձությունները, կամ 2011թ. փետրվար–մարտ ամիսներին արաբական խռովությունների աջակցությունը կոչվել են «կիբեռպատերազմ»՝ փաստորեն ակնարկելով, որ պատերազմի հայեցակարգն այլևս չի սահմանափակվում միայն ազգային պետությունների շրջանակով։ Ընդհանուր սահմանման բացակայության պայմաններում ԵՄ անդամ երկրները և Եվրոպական հանձնաժողովը հետևողականորեն խուսափել են պաշտոնական փաստաթղթերում «կիբեռպատերազմ» եզրույթի օգտագործումից՝ փոխարենը գերադասելով այնպիսի չեզոք ձևակերպումներ, ինչպիսիք են «կիբեռլրտեսություն», «կիբեռհարձակում» կամ «կիբեռպաշտպանություն»* (European Parliament, 2012, p. 9)։

2.1 Կիբեռպատերազմի տարբեր մակարդակները

Այսպես կոչված *AF-SAB* մոդելի համաձայն՝ գոյություն ունի կիբեռհարձակումների երեք աստիճան։

Առաջին աստիճանի կիբեռհարձակումները «ցանցային պատերազմներն» են կամ *«համակարգային ադմինիստրատորն ընդդեմ համակարգային ադմինիստրատորի»:* Այստեղ կիրառվում են «վնասաբեր տրամաբանություն», «Տրոյական» հարձակումներ, կեղծարարությամբ անձնական գաղտնի տվյալների ձեռքբերում (*phishing*), ծրագրերի հայտնի խոցելի տեղերի շահագործում, համացանցային կայքերի այլափոխում և այստեղ տեղ գտած անհարմարություններ պատճառող այլ գործողություններ: Այս կարգի հարձակումների բնույթն այնքան էլ լուրջ չէ, ինչպես, օրինակ՝ որոշ պետությունների ենթադրաբար հովանավորած «*Moonlight Maze» և «Titan Rain»* արշավները ԱՄՆ կառավարության դեմ: Այդ հարձակումներից կարելի է պաշտպանվել ցանցային անվտանգության պատշաճ միջոցների կիրառման օգնությամբ (*European Parliament,* 2012, p. 7): *«Titan Rain»*-ը կատարելագործված կիբեռլրտեսական հարձակում էր, որը *«սկսվեց 2003թ. ԱՄՆ-ի դեմ և բերեց ԱՄՆ կառավարական և ռազմական գաղտնի համակարգերի լայնամասշտաբ ճեղքման՝ հանգեցնելով 10-12 տեռաբայթ ծավալով տեղեկությունների կորստյան» (European Parliament,* 2012, p.52): Այս և մյուս հարձակումները կազմակերպել և իրականացրել էին պետության հետ առնչություն չունեցող չինացի համակարգչային ցանցահեները: Չորս տարվա ընթացքում նրանք նմանատիպ հարձակումներ գործեցին նաև ԵՄ անդամ երկրների և ԵՄ հաստատությունների պետական կառավարման համակարգերի վրա: Թեև հարձակվողներն ուղղակի առնչություն չունեին չինական պետության հետ, սակայն նրանք, հավանաբար, համագործակցում էին չինական անվտանգության ծառայությունների պաշտոնական հրամանատարության հետ, որն իր հերթին կապեր ունի Չինաստանի բարձրաստիճան քաղաքական ղեկավարությունում:

Երկրորդ աստիճանի կիբեռհարձակումները պատկանում են «կիբեռօգնությամբ կինետիկ մարտ» տեսակին: Օպերատորը փոր-

ձում է հասնել «կինետիկ էֆեկտի», ավանդական հարձակման, օրինակ՝ օդային հարվածի հետ համակցությամբ: Այսպես, օպերատորը կիրառում է համակարգչային «վնասաբեր տրամաբանություն»՝ օդային պաշտպանության համակարգը վնասազերծելու համար: Այս օրինակը ներկայացնում է 2-րդ աստիճանի կիբեռհարձակում (*European Parliament,* 2012, pp. 7-8): 2008թ. տեղի ունեցած կիբեռհարձակումները Վրաստանի վրա նույնպես դասվում են այս կարգին: Դրանք ուղեկցվում էին ավանդական ռազմական գործողություններով և հետևապես՝ ունեին կինետիկ էֆեկտ: Վրաստանի դեմ պատերազմում ռուսներն այլակերպում էին համացանցային կայքերը՝ միաժամանակ հարձակումներ գործելով նաև կենսական նշանակություն ունեցող էներգետիկ ենթակառուցվածքների վրա: Երկրորդ աստիճանի կիբեռպատերազմի մեկ այլ օրինակ են 2007թ. Սիրիայի և Իսրայելի միջև տեղի ունեցած գործողությունները, երբ իսրայելցիները կիրառեցին *«Senior Suter»* կոչվող ամերիկյան կիբեռզինատեսակը՝ սիրիական հակաօդային պաշտպանության ցանցը վնասազերծելու համար, և հաջողությամբ օդային հարվածներ հասցրին Սիրիային՝ ճշգրիտ ռմբակոծելով ենթադրյալ միջուկային օբյեկտները:

Վերջին՝ երրորդ աստիճանը «չարամիտ մանիպուլյացիան» է, որը մասնագետների կողմից համարվում է ամենավտանգավոր հարձակումը: Այս հարձակումներից *«պետք է առավել զգուշանալ: Դրանք կատարվում են ծածուկ, նախապես պլանավորված ու կազմակերպված են և կարող են լայնամասշտաբ խառնաշփոթ ու խաթարումներ առաջացնել, ընդ որում, զոհերը չեն էլ պատկերացնում, որ իրենց պրոբլեմները հարուցված են կիբեռմիջոցներով»:*

Համաձայն Եվրոպական խորհրդարանի ծառայությունների հրապարակած մի հետազոտության՝ *«3-րդ աստիճանի հարձակումների տակ նաև թաքնված է լինում հնարավոր վարքագծերի մի մեծ շարք, որը կարող է ներառել աղյուսակային ֆայլի պարզ մանիպու-*

լյացիայից մինչև Stuxnet և նմանատիպ այլ սահմանափակ բնույթի կանխամտածված հարձակումներ որևէ կենսական ենթակառուցվածքի վրա, մեծաթիվ զոհեր հարուցող հարձակումներ ողջ պետության կենսական նշանակության ենթակառուցվածքների վրա կամ նույնիսկ համացանցն ամբողջությամբ հունից շեղելու գործողություններ» (*European Parliament,* 2012, p. 8)։

Ընդգծենք, որ *«Stuxnet»*-ի տակ մենք նկատի ունենք այն «կիբեռհրթիռը», որն *«անմիջականորեն ուղղված էր Իրանի միջուկային ծրագրի դեմ՝ որպես հարվածի թիրախ ընտրելով ուրանի հարստացման կարողությունները* (*European Parliament,* p. 52, *The Economist,* 2010)։ Ինչպես նշվում է Եվրոպական խորհրդարանի զեկույցում. *«անհերքելի ապացույցներ կան, որ Stuxnet-ի միջոցով հաջողվել է վնաս հասցնել Իրանում ուրանի հարստացման ծրագրին և հետաձգել այն* (*European Parliament,* 2012, p. 52, *Farwell and Rohozinski,* 2011, pp. 23-40)։ Այս հարձակումն առաջինը չէր, որում կիրառվեց բարձր տեխնոլոգիաների «անտեսանելի» զենքը։ Ինչպես պնդում է ԱՄՆ նախկին նախագահ Ռոնալդ Ռեյգանի խորհրդատու Թոմաս Ռիդը, ԿՀՎ-ն 1982թ. «լոգիստիկ ռումբ» է կիրառել սովետական մի խողովակաշար ոչնչացնելու համար։ Նրա խոսքերով. *«Այն ծրագրավորված էր այնպես, որ խելակորույս արագության հասցնի պոմպերի պտույտները և խառնի փականների կարգավորումները՝ ստեղծելով խողովակաշարի հանգույցների ու զոդվածքների դիմադրողականության համար անտանելի ճնշումներ։ Արդյունքում՝ ստացվեց ոչ միջուկային բնույթի այնպիսի վիթխարի հզորության մի պայթյուն և հրդեհ, որպիսին երբևէ հնարավոր է եղել դիտել տիեզերքից»* (*Reed,* 2004, p. 269)։

2.2 Ամերիկյան գերիշխանությունը

Ակնհայտ է, որ ԱՄՆ-ը համարվում է կիբեռպատերազմի և կիբեռպաշտպանության գծով առաջատար պետություն։ Արդեն հիշա-

տակված դեպքերից բացի նշենք նաև, որ 1991թ. իրաքյան պատերազմի ժամանակ ԱՄՆ-ը տպավորություն գործեց միջազգային հանրության վրա կիբեռպատերազմի իր կատարելագործված հմտություններով: Տարիներ անց, 2010թ., ՆԱՏՕ-ն ԱՄՆ առաջնորդությամբ առաջին կազմակերպությունն էր, որ գիտակցեց կիբեռհարձակումներից բխող «նոր սպառնալիքներին» հակազդելու անհրաժեշտությունը: Այդ անհրաժեշտությունն առավել ակնհայտ դարձավ 2007թ. Էստոնիայի դեմ կատարված հարձակումից հետո, որը ներառում էր համացանցային վանդալիզմ: Մասնավորապես, երեք շաբաթվա ընթացքում հարձակում գործողները խաթարեցին Էստոնիայի հանրային ծառայությունների և բանկային համակարգի աշխատանքը: Ամենայն հավանականությամբ, հարձակվողները ռուսաստանցի ցանցահեներ էին: Հարձակումը հզոր ցնցում էր միջազգային հանրության համար: Այս իրադարձությունը զգաստացրեց շահագրգիռ կողմերին և ՆԱՏՕ-ին ստիպեց համապատասխան որոշումներ ընդունել և վերանայել իր ռազմավարական պաշտպանական հայեցակարգը: 2010թ. նոյեմբերին կայացած Լիսաբոնի գագաթաժողովին ՆԱՏՕ-ն ստեղծեց «Կիբեռպաշտպանության կառավարման մարմինը» (*Cyber Defence Management Authority (CDMA)*, որի իրավասությունների մեջ մտնում են դաշինքի ներսում կիբեռպաշտպանության հետ կապված որոշումների համակարգումն ու ձևավորումը (*European Parliament,* 2012, p. 26, NATO 2010a): Չինաստանն ու Ռուսաստանը նույնպես ներգրավված են կիբեռպատերազմի բոլոր աստիճաններում, քանի որ չունեն ուրիշ այլընտրանք, քան արդի դարաշրջանի պահանջներին արձագանքելը՝ սեփական շահերին ծառայելու և դրանք պաշտպանելու համար ձեռնարկելով բոլոր հնարավոր կանխարգելիչ միջոցառումները: Իրականում նրանք ոչ միայն պաշտպանվում են, այլև հետևում են ագրեսիվ քաղաքականության: Այս կապակցությամբ կիբեռհարձակումները հարկ է դիտարկել քաղաքական գործելակեր-

պերի պրիզմայի միջով: Այստեղ կարելի է ընդգծել, որ կիբեռպատերազմների քանակական վերլուծությունում չի կարելի կենտրոնանալ բացառապես երեք վերոհիշյալ աստիճանների վրա, այլ պետք է դիտարկել նաև քաղաքացիական, առևտրատնտեսական, վարչական, բանկային և ռազմական ոլորտները, որոնք սովորաբար կիբեռհարձակումների թիրախ են դառնում: Այս իմաստով, նման կիբեռառևտրատնտեսական պատերազմ ներկայումս ընթանում է Չինաստանի և ԱՄՆ-ի միջև: ԱՄՆ Կոնգրեսի համար պատրաստված «Չինաստան–ԱՄՆ առևտրային խնդիրները» վերնագրով զեկույցի կապակցությամբ Ուեյն Մ. Մորիսոնը նկատել է. *«ԱՄՆ բազմաթիվ վերլուծաբաններ և քաղաքական գործիչներ պնդում են, որ Չինաստանի կառավարությունը ԱՄՆ ֆիրմաների հանդեպ ուղղված կիբեռտնտեսական լրտեսության հիմնական պատվիրատուներից մեկն է: Օրինակ, Ներկայացուցիչների պալատի հետախուզության հարցերով մշտական հատուկ կոմիտեի նախագահ, ներկայացուցիչ Մայք Ռոջերսը 2011թ. հոկտեմբերի 4-ին կայացած լսումներում հայտարարել է, որ այս կարգի լրտեսությունն ինչ–որ մեկին վերագրելը հեշտ չէ, սակայն եթե լսենք մասնավոր հատվածը ներկայացնող կիբեռվերլուծաբաններին, ապա նրանց պնդմամբ՝ կասկած չի հարուցում, որ այս զանգվածային արշավն իրականացվում է չինական կառավարության կողմից: Չեմ կարծում, թե պատմությանը հայտնի է մեկ այլ նախադեպ, երբ հետախուզության այսքան զանգվածային ու հետևողական ջանքեր են գործադրվել երբևիցե որևէ պետության կողմից՝ այսպես անթաքույց կերպով կոմերցիոն տվյալներ և մտավոր սեփականություն գողանալու համար: Չինաստանի կողմից իրականացվող տնտեսական լրտեսությունը հասել է անտանելի աստիճանի, և, իմ կարծիքով, Միացյալ Նահանգներն ու Եվրոպայի և Ասիայի մեր դաշնակիցները պարտավոր են հակազդեցություն ցուցաբերել Պեկինին և պահանջել դադարեցնել այս ավազակությունը»:*

ԱՄՆ Ազգային հետախուզության տնօրենի գրասենյակի պատրաստած զեկույցի տվյալներով՝ *«չինացիները տնտեսական լրտեսության աշխարհի ամենաակտիվ և հետևողական դերակատարներն են: ԱՄՆ մասնավոր հատվածի ձեռնարկությունների և կիբեռանվտանգության մասնագետների հաղորդմամբ՝ բարձրացել է համակարգչային ցանցերի ներխուժումների մի ալիք, որի սկզբնաղբյուրը Չինաստանում է, սակայն հետախուզական հանրությունը չի կարող հաստատել, թե ով է դրա պատասխանատուն»:* Այնուհետև զեկույցում նախազգուշացում է հնչում, որ *«Չինաստանը շարունակելու է առաջնորդվել արևմտյան տերություններին «հասնելու և անցնելու» իր վաղեմի քաղաքականությամբ: Չինական և ամերիկյան ընկերությունների միջև զարգացող համագործակցությունը, ինչպիսին է, օրինակ, չինացի տեխնիկական փորձագետների աշխատանքը ԱՄՆ օբյեկտներում և ԱՄՆ արտադրության և հետազոտական ու մշակման աշխատանքների արտապատվիրումը Չինաստանում, չինական պետական գործակալություններին և մասնավոր բիզնեսին ԱՄՆ-ի մասին զգայուն բնույթի տնտեսական տեղեկություններ հավաքելու հնարավորություններ է ընձեռում (Morrison,* 2012, p. 33):

2.3 Չինաստանը, Ռուսաստանը և ցանցահենների բանակը

Չինաստանը և Ռուսաստանն արտոնյալ դիրքեր են զբաղեցնում գլոբալ կիբեռտերությունների շարքում և ունեն հատկապես ԱՄՆ շահերի դեմ գործող համակարգչային ցանցահենների հսկա բանակներ: Ցանցահենների մեծամասնությունը ոչ մի պաշտոնական կապ չունի չինական կամ ռուսական կառավարությունների հետ: Սակայն բոլորին հայտնի «գաղտնիքն» այն է, որ չինական կառավարությունը լռելյայն հավանություն է տալիս ցանցահենների հարձակումներին: «Ինտեգրված ցանցային էլեկտրոնային պատերազմ» վերնագրով կիբեռպատերազմի չինական հայեցակարգը նմանվում է ամերիկյան

«Ցանցային էլեկտրոնային պատերազմին»: Այս համատեքստում քաղաքացիական ռեսուրսները («պատերազմող ժողովուրդը») մոբիլիզացվում են, որպեսզի փորձ կատարվի գործողություններ իրականացնել հակամարտության ռազմավարական մակարդակում, այսինքն՝ «տեղեկատվական պատերազմում»: Տեղեկատվական այս պատերազմը բաժանվում է երեք կարգի՝ ՋԼՄ պատերազմ, հոգեբանական պատերազմ և իրավական պատերազմ (*European Parliament,* p. 55): Չինացիներն ունեն պաշտպանողական և հարձակողական կարողությունների մի շատ հզոր համակարգ, իսկ իրական բանակը՝ «հայրենասեր ցանցահեները», պատասխանատու են արևմտյան պետությունների և նրանց շահերի դեմ ձեռնարկվող հարձակումների համար: «Կարմիր ցանցահենների դաշինքը» հարձակողական գործողություններ իրականացնողների ամենամեծ ակումբն է՝ 400 հազ. անդամ: Պենտագոնը ստիպված էր հատուկ միջոցներ ձեռնարկել նրանց հարձակումները կանխարգելելու համար (*European Parliament,* 2012, p. 57):

Նույն կերպ, Ռուսաստանը մեծ ուշադրություն է հատկացնում ԱՄՆ ցանցահեններից իր քաղաքացիական հասարակությունը, ռազմական/պետական ենթակառուցվածքները և ապարատը պաշտպանելուն ուղղված միջոցների ու միջոցառումների վրա: «Փափուկ և խելամիտ» ուժի իմաստով ԱՄՆ-ը ձգտում է ներգործել Ռուսաստանի հանրային կարծիքի և, ավելին, որոշումների կայացման գործընթացի վրա (*Nye,* 1991; *Nye,* 2004, pp. 2, 34-35, 44-45; 2006; *Crocker et al,* 2007, p.13; *Etheridge,* 2009): Այս ռազմավարությունը կոչվում է «ռեֆլեքսիվ վերահսկողություն»: Ըստ այդ հայեցակարգի, *«թշնամիներից մեկը մյուսին է փոխանցում որոշումների կայացման պատճառներն ու հիմքերը» (Thomas,* 2004): Սա ռազմավարական մեթոդ է, որի միջոցով ԱՄՆ-ը ազդեցություն է գործում ինքնակալական ռեժիմների ճնշման տակ գտնվող հանրային որոշ կարծիքների վրա՝ հանրությանը մղե-

լով ապստամբության: Իրանը և արաբական գարունը ԱՄՆ կիբեռ-պատերազմական ծառայությունների կողմից ռազմավարական այս մեթոդի կիրառման առավել ակնհայտ օրինակներից են: Ճնշումների ենթարկվող հանրության կողմից որոշումների կայացման գործընթացի վրա ազդեցություն գործող ամբողջ անհրաժեշտ ինֆորմացիան, պատճառաբանությունները և տվյալները տարածվում էին կիբեռտարածության միջոցով: Իհարկե, «խելամիտ ուժի» ռազմավարական հայեցակարգին բնորոշ այս մեթոդի կիրառման արդյունքները ոչ միշտ են դրական լինում: ԱՄՆ-ի կողմից արտերկրների հանրային կարծիքների վրա թողած ազդեցությունից բացի, հասարակությունում և ավտորիտար քաղաքական համակարգերում առկա են նաև այլ գործոններ, որոնք անդրադառնում են որոշումների կայացման գործընթացի վրա: Ռազմավարական նպատակին հասնելն ավելի դյուրին է, երբ արտերկրի հանրային կարծիքը պատրաստ է ընկալել համացանցով տարածվող քարոզչությունը: Նման քաղաքականության հաջողությունը կամ տապալումը նաև կախված է ԱՄՆ-ի կողմից հարձակման ենթարկվող պետության հատուկ ծառայություններ-ի կարողություններից: Հարցն այն է, թե որքանով են նրանք արդյունավետ հակազդում նման «կիբեռպատերազմական զորավարժություններին»: Զարմանալի չէ, որ Ռուսաստանի տեղեկատվական դոկտրինը կենտրոնացած է հանրային կարծիքի պաշտպանության և ռուսական «հոգևոր վերածննդի» վրա՝ ստեղծելով «տեղեկատվա-հոգեբանական» և «տեղեկատվա-տեխնիկական» միջոցների բաժանմունքներ (*Bikkenin,* 2003):

3. Դարակազմիկ իրադարձությունը

«Վիքիլիքսի գործը», ամերիկյան հազարավոր գաղտնի փաստաթղթերի հրապարակումը, որը հայտնի է նաև որպես «Քեյբլգեյթս», երևան հանեց նոր դարաշրջանի կատարելագործված բնույթը՝ դարաշրջան,

որում տեխնոլոգիան առաջնային գործիք է հանդիսանում գաղտնի ծառայությունների կամ անհրաժեշտ հմտությունների տիրապետող որևէ այլ անձի կամ կազմակերպության համար: Հույժ գաղտնի բազմաթիվ փաստաթղթերի (251287 դիվանագիտական հաղորդագրությունների) հրապարակումը լույս սփռեց գաղտնի դիվանագիտության մութ կողմերի վրա և ցուցադրեց, թե դիվանագետներն ինչպես են գնահատում միմյանց անդրկուլիսյան խոսակցություններում (*WikiLeaks*, 2012): 2010թ. օգոստոսի 20-ին շվեդական դատախազությունը «Վիքիլիքս»-ի հիմնադիր Ջուլիան Ասանժին ձերբակալելու հրաման արձակեց՝ երկու մեղադրանքով: Մեկը բռնաբարության մեղադրանք էր, իսկ մյուսը՝ սեռական ոտնձգությունների: Ասանժը հերքում է մեղադրանքները՝ պնդելով, որ ինքը դարձել է զրպարտության զոհ: Շվեդական իշխանությունները Մեծ Բրիտանիայից պահանջում են հանձնել Ասանժին, որը թաքնվում է այդ երկրում Էկվադորի դեսպանատանը: Ասանժը քաղաքական ապաստանի խնդրանքով դիմել է Էկվադորի դեսպանություն, և էկվադորյան իշխանությունները 2012թ. օգոստոսի 16-ին դրական որոշում են ընդունել այդ կապակցությամբ, որը Բրիտանիայի հետ դիվանագիտական միջադեպի առիթ է հանդիսացել: Էկվադորի արտաքին գործերի նախարարը հայտարարել է, որ իր երկիրը ապաստան է տվել Ասանժին, «քանի որ նրան հանձնելու դեպքում նա քաղաքական հետապնդումների կենթարկվի» (Lai, 2012): Բրիտանական կառավարությունը հստակ է արտահայտվել նրան ձերբակալելու և Շվեդիային հանձնելու իր մտադրությունների մասին: Ասանժը երկյուղում է, որ շվեդական իշխանություններն իրեն կուղարկեն ԱՄՆ, որտեղ նա կարող է մահվան դատապարտվել: ԱՄՆ իշխանությունները մեղադրում են նրան հույժ գաղտնի հաղորդագրությունները (ամերիկյան պաշտոնական փաստաթղթերը) հրապարակելու մեջ, ինչը ռիսկի է ենթարկել երկրի անվտանգությունը: 2012թ. օգոստոսի 14-ին արդարացնելով երկու օր անց կայացվելիք

դրական որոշումը՝ Էկվադորի նախագահ Ռաֆայել Կոռեան հայտարարեց. «Շվեդիայում գործընթացը քննման կարիք ունի, հարկ է հաշվի առնել ԱՄՆ-ին հանձնելու հավանականությունը, և եթե այնտեղ գաղտնի տրիբունալ կա, ապա մահվան դատավճիռ կայացնելու ռիսկ գոյություն ունի՞ արդյոք: Այս ամենը պահանջում է մեծածավալ տեղեկությունների, միջազգային օրենքների վերլուծություն, որպեսզի կայացվելիք որոշումը հիմնված լինի հավաստի ինֆորմացիայի վրա, կրի բացարձակապես պատասխանատու և ինքնիշխան բնույթ» (*Correa*, 2012, մեջբերումը՝ *CNN Wire Staff*, 2012):

«Վիքիլիքսը» ստվեր նետեց ԱՄՆ անվտանգության համակարգի վրա և նվաստացրեց ամերիկյան գաղտնի ծառայություններին: Փաստորեն, սա դարակազմիկ գործ էր, որն ի ցույց հանեց տեխնոլոգիայի նշանակությունը միջազգային հարաբերություններում և նոր տիպի պատերազմները, որոնք անաղմուկ ընթանում են ոչ միայն պետությունների միջև, այլև պետությունների և ոչ պետական դերակատարների միջև: Այս դեպքում մենք վկա ենք դարձել, թե ինչպես տեխնոլոգիան վերացնում է գերտերության և մասնավոր էլեկտրոնային ԶԼՄ-ի միջև եղած հզորության տարբերությունը:

Եզրակացություններ

Տեխնոլոգիան հզորության կառուցվածքային բաղադրիչ գործոն է, որը պետությունների կողմից ծառայեցվում է իրենց ազգային շահերին՝ առևտրատնտեսական կիբեռպատերազմի համատեքստում: Նման պատերազմներ ընթանում են ԱՄՆ-ի և Չինաստանի, ԱՄՆ-ի և Ռուսաստանի միջև՝ չբացառելով նաև, որ դրանցում ընդգրկվում են այլ երկրներ ևս: Սա միջազգային համակարգի տիտանների կռիվ է, որտեղ ԱՄՆ-ը խաղում է Զևսի դերը: Ավելին, տեխնոլոգիան և կիբեռպատերազմը կիրառվում են նաև ավանդական պատերազմների և ահաբեկչության դեմ պատերազմի շրջանակներում: Իրականում այն առևտրա-

տնտեսական և կիբեռնետիկ պատերազմների համակցություն է, որում իր արտացոլումն է գտնում արդի դարաշրջանը: Այն ցույց է տալիս, թե որքան բարդ են միջազգային հարաբերությունները ներկա ժամանակաշրջանում: Ակնհայտ է, որ առկա են «երկու կամ երեք տեսակի պատերազմներ», ընդ որում, մեկն ընթանում է մյուսի շրջանակներում՝ առանց ավանդական, դասական ռազմի միջոցների կիրառման: Մասնավորապես, բանակն օգտագործում է կիբեռմեխանիզմները որպես լրտեսության անփոխարինելի գործիքներ՝ ազգային շահերի պաշտպանությանը և առաջխաղացմանը նպատակաուղղված համընդհանուր ռազմավարական ծրագրի շրջանակում: Զուգահեռաբար, կիբեռպատերազմի գործիքներն ու զենքերը կիրառվում են նաև սովորական պատերազմներում: Առաջադեմ տեխնոլոգիան մշտապես կարևորագույն նշանակություն ունի միջազգային դերակատարների համար՝ հաղթանակն ապահովելու նկատառումով:

Միջազգային համակարգը թևակոխել է նոր դարաշրջան, որում կառուցվածքային փոփոխություններ են ընթանում և իշխանությունը գոյակցում է տեխնոլոգիական առաջընթացի և կարողությունների հետ: Գերտերությունների՝ ԱՄՆ-ի, Չինաստանի, Ռուսաստանի միջև ընթանում է անտեսանելի կիբեռպատերազմ: Անշուշտ, գերտերություններից բացի, մյուս երկրները նույնպես արդեն ներգրավվել են կիբեռպատերազմում, որի համար ձևավորվել են նոր տիպի բանակներ: Այժմ համակարգչային ցանցահեները խաղում են «ժամանակակից զինվորների» դերը՝ դրանով իսկ բացահայտելով տեխնոլոգիայի ծայրաստիճան կարևորությունը՝ որպես պետության հզորության անփոխարինելի գործոն (*Dougherty and Pfaltzgraff,* 1992, p. 116): Այս իրողությունում պատերազմի կառուցվածքը և մեթոդները փոփոխվելու միտում ունեն, ինչը վերաբերում է նաև միջազգային համակարգի կառուցվածքին, որտեղ ազգային պետությունները դեռևս շարունակում են գերիշխող դիրքեր պահպանել: Այնուամենայնիվ, շուկանե-

րը, ինչպես նաև «Ալ Քաիդայի» կարգի ահաբեկչական կազմակերպությունները ջանք չեն խնայում գերիշխող պետություններին փոխարինելու համար: «Վիքիլիքսի» գործի պրիզմայի միջով երևան է գալիս մի նոր քաղաքական երևույթ, որը բխում է տեխնոլոգիայից և արտացոլում վերջինիս աճող նշանակությունը, ինչպես նաև միջազգային համակարգում տեղի ունեցող փոփոխությունները, որտեղ ոչ պետական էլեկտրոնային ՋԼՄ հանդիսացող կազմակերպությունը կիբեռպատերազմի մեջ է ներգրավվում ԱՄՆ-ի հետ: Ցայսօր ԱՄՆ պարտությունն այդ պատերազմում ակնհայտ է: Այս իրադարձությունը հիշեցնում է Դավիթի և Գողիաթի հայտնի պատմությունը: Այսպիսով, պատմությունը կրկնվում է՝ արդեն ուրիշ միջոցների կիրառության պարագայում: Այն ժամանակ դա քարն ու պարսատիկն էին, իսկ այսօր՝ տեխնոլոգիան:

Մայիս, 2013թ.

Աղբյուրներ և գրականություն

1. *Almasmari, H., Jamjoom M. and Abedine S.* (2012) *Yemen: Al Qaeda affiliate behind blast that killed 101 soldiers.* CNN. May 22. Available from: http://articles.cnn.com/2012-05-22/middleeast/world_meast_yemen-violence_1_al-qaeda-al-sharia-president-saleh?_s=PM:MIDDLEEAST
2. BBC News (2012) *Muslim Brotherhood's Morsi declared Egypt president, June 24.* Available from: http://www.bbc.co.uk/news/world-18571580
3. *Bjelopera, P. J.* (2011) *American Jihadist Terrorism: Combating a Complex Threat.*Congressional Research Service. November 15. Available from: http://www.fas.org/sgp/crs/terror/R41416.pdf
4. *Bin Laden, O.* (2005) Interview *Message to the World*, Verso, October 21, 2001.
5. *Blanchard, C.* (2007) *'Al Qaeda: Statements and Evolving Ideology'.* CRS Report for Congress. July 9. Available from: http://www.fas.org/sgp/crs/terror/RL32759.pdf
6. Centre for Defence Information. *Operation "Enduring Freedom"*. Washington. Available from: http://www.cdi.org/program/issue/index.cfm?ProgramID=39&issueid=48

7. *CNN News* (2012), Breaking News. *The speech that President Assad addresses the Syrian Parliament.* 3 June.
8. *CNN News* (2012a), *Kofi Annan resigns as envoy to Syria.* Available from: http://security.blogs.cnn.com/2012/08/02/kofi-annan-resigns-as-envoy-to-syria/
9. *CNN News* (2012b), A reportage on the TV (CNN International) which transmitted the message sent by the Syrian rebels of the "Syrian Liberate Army". The rebels called upon Turkey to military intervene.
10. *CNN News* (2012c), *Muslim Brotherhood's Morsi declared Egypt's new president*. June 24. Available from: http://edition.cnn.com/2012/06/24/world/africa/egypt-politics/index.html?hpt=hp_t1
11. *Correa, R.* (2012) Cited in CNN wire staff. Ecuador: *Decision on WikiLeaks founder's asylum request coming.* August 14. Available form: http://www.cnn.com/2012/08/14/world/americas/ecuador-assange/index.html
12. *Charalambides, Y.* (2011) *Cyprus Issue: Diplomatic Plots, top secret documents and testimonies from 1950 to 2010, Strategic deficits and options.* Athens: Piotita.
13. *Charalambides, Y.* (2013) *The Third World War, Global Titans and Sworn Soldiers*. ERPIC, Nicosia.
14. *Clarke, R A.* (2010) *Cyber War. The Next Threat to National Security and What to Do About.* As imprint of HarperCollins Publishers.
15. *Crocker, A., Hampson, O. and Aall P.* (2007) *Leashing the Dogs of War: Conflict Management in a Divided World*. US Institute of Peace Press.
16. *Dougherty, J. and Pfaltzgraff R.* (1992) *Contending Theories of International Relations: A Comprehensive Survey*. Athens: Papazisis Publications, vol. 1.
17. *Economist* (2010) *"Cyberwar: War in the Fifth Domain".* 1 July. Available From: http://www.economist.com/node/16478792
18. *European Parliament* (2012) External Representation of the Euro Area. Directorate General for International Policies Policy A: Economic and Scientific Policy. A Study issued from the European Parliament. Authors: Alessandro Giovannini.
19. *Daniel Gros, Paul Ivan, Piotr Maciej Kacznski, Iego Valiante.* Available from: http://www.europarl.europa.eu/studies
20. *Elsea, Jeniffer K.* (2007) *Treatment of "Battlefield Detainees" in the War on Terrorism.*Updated January 23, 2007. CRA Report for Congress, order code RL 31367. Available from: http://www.fas.org/sgp/crs/terror/RL31367.pdf
21. *Etheridge, E.* (2009) *How 'Soft Power' Got 'Smart'. The New York Times*. January 14. Available from: http://opinionator.blogs.nytimes.com/2009/01/14/how-soft-power-got-smart/
22. *Farwell, J. and Rohozinski R.* (2011). *'Stuxnet and the Future of Cyber War'.* Survival, Vol. 53(1), 2011.
23. *Gilpin, R.* (1981) *War and Change in World Politics*, Cambridge University Press, New York.

24. *Ifestos, P. and Platias A.,* (1992) Greek Preventive Strategy. Published by Papazisis, Athens.
25. *Karl, M.* (1955) *The Poverty of Philosophy. Answer to the Philosophy of Poverty by M. Proudhon.* Progress Publishers. First Publication in Paris and Brussels 1847. Available from: http://www.marxists.org/archive/marx/works/download/pdf/Poverty-Philosophy.pdf
26. *Katzman, K.* (2005) *Al Qaeda: Profile and Threat Assessment*. - CRS Report for Congress. Received through the CRS Web. August 17. Available from: (http://www.fas.org/sgp/crs/terror/RL33038.pdf)
27. *Lai, A.* (2012) *Timeline: Julian Assange's extradition battle*. CNN. August 16. Available from: http://www.cnn.com/2012/08/16/world/europe/assange-extradition-timeline/index.html?iid=article_sidebar
28. *Lecker, M.* (2008*) "The 'Constitution of Medina': Muhammad's First Legal Document". Journal of Islamic Studies* 19 (2): 251–253, DOI:10.1093/jis/etn021. Available from: http://jis.oxfordjournals.org/content/19/2/251
29. *Lynn, W. J. III* (2010) *"Defending a New Domain: The Pentagon's Cyberstrategy*". *Foreign Affairs*, Sept/Oct. 2010.
30. *Morgenthau, H.* (1978) *Politics among Nations: The Struggle for Power and Peace*. New York: Knopf.
31. *Morisson, M.W.* (2012) *China-U.S. Trade Issues China-U.S. Trade Issues.* Congressional Research Service. May 21. Available from: http://www.fas.org/sgp/crs/row/RL33536.pdf
32. NATO (2011) *Defending against cyber attacks*. NATO Homepage. Available from: http://www.nato.int/cps/en/natolive/topics_49193.htm
33. *Nye, J.* (1991) *Bound to Lead: The Changing Nature of American Power*. US: Basic Books
34. *Nye, J.* (2004) *Soft Power: The Means to Success to World Politics*, U.S: Public Affairs
35. *Nye, J.* (2006) *In Mideast, the Goal is "Smart Power". Boston Globe*. August 19.
36. Available from: http://www.boston.com/news/globe/editorial_opinion/oped/articles/2006/08/19/in_mideast_the_goal_is_smart_power/
37. *Reed, T.* (2004) *At the Abyss: An Insider's History of the Cold War*. New York, Press.
38. *Tomas, T.* (2004) *"Comparing US, Russia and Chinese Information Cooperation Concepts"*. Foreign Military Studies Office, February. Available from: http://www.dodccrp.org/events/2004_CCTS/CD/papers/064.pdf.
39. *The Economist,* (2010) *A cyber-missile aimed at Iran?* 24 September. Available from: http://www.economist.com/blogs/babbage/2010/09/stuxnet worm.
40. *Wikileaks* (2012), *Secret US Embassy Cables.* Available from: http://wikileaks.org/cablegate.html#

НЕВИДИМАЯ КИБЕРВОЙНА

Янос Хараламбидис

Резюме

В статье обсуждается важность технологий в современную эпоху, в частности в контексте войны нового типа – кибервойны. Война этого типа соответствует происходящим в международной системе структурным изменениям, в которых технологии играют особую роль. Проанализированы разные типы войн, предпринята попытка сформулировать понятие «кибервойна» и объяснить ее практическое осуществление. Обсуждается воздействие кибервойны на развитие международной системы и произошедшие вследствие этого структурные изменения, а также та важная роль, которую играют на международной арене кибервойны и технологии.