

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԻ ՔԱՆԻ ՀԱՐՑԵՐ

Մամվել Մարտիրոսյան

Հոդվածում դիտարկվում են նորագույն տեխնոլոգիաների ազդեցության աճի հետ կապված պետության առջև հառնող տեղեկատվական անվտանգության հարցեր: Մասնավորապես ներկայացվում է Հայաստանի տեղեկատվական տեխնոլոգիաների ոլորտի արդի իրավիճակը՝ այլ պետությունների համեմատությամբ:

Տեղեկատվական անվտանգության մեկ այլ ուղղությունը, որ դիտարկվում է հոդվածում, վերաբերում է թշնամաբար տրամադրված պետությունների և սոցիալական խմբերի ագրեսիվ գործողություններին, որոնք նորագույն տեխնոլոգիաներ են կիրառում Հայաստանի և հայության դեմ քարոզչություն վարելու համար: Հայաստանը և հայությունը հայտնվել են տեղեկատվական լուրջ պատերազմին դեմ-հանդիման, որը վարում են սահմանակից պետությունները: Հոդվածում անվտանգության հարցերը դիտարկվում են ինչպես պետության ու պետական մարմինների, այնպես էլ հասարակության և զանազան սոցիալական ցանցերի տեսանկյունից:

Ներածություն

Այսօր տեղեկատվական տեխնոլոգիաների ազդեցության աննախադեպ գլոբալ աճի պայմաններում այս ոլորտի անվտանգությունը դառնում է առանձին երկրների գոյատևման հիմնական խնդիրը: Պետությունների կախվածությունը տեղեկատվական տեխնոլոգիաներից (SS) տարեցտարի մեծանում է, ընդ որում՝ ոլորտին առնչվող խնդիրներն էլ ավելի են գլոբալացվում, ջնջվում են սահմանները: Հետևաբար, տեղեկատվական անվտանգության նկատմամբ ուշադրությունը Հայաստանի համար կենսականորեն կարևոր անհրաժեշտություն է:

Նշենք հետևյալ ոլորտները, որոնք իրական մարտահրավերներ են ներկայացնում Հայաստանի տեղեկատվական անվտանգությանը.

1. Տեղեկատվական ցանցերում պետության ներկայացված լինելու հնարավորությունները և այդ ուղղությամբ աջակցությունը ոչ պետական կառույցներին, թշնամական քարոզչությանը դիմակայելու և դրական իմիջ ձևավորելու հնարավորությունները:

2. Տեղեկատվական ինքնիշխանության հանդեպ այլ պետությունների և ցանցային խմբերի ագրեսիվ քաղաքականությանը դիմակայելու պետության կարողությունը:
3. Ինչպես ներքին, այնպես էլ արտաքին հարթությունում տեղեկատվական տեխնոլոգիաները կիրառելու երկրի ներուժը:

Բոլոր այս ոլորտները փոխկապակցված են և ենթադրում են թե՛ պետական կենտրոնացված մոտեցում և թե՛ զանազան ցանցային խմբերի ներգրավվածություն, որոնք ի վիճակի են վարել ինքնուրույն քաղաքականություն տեղեկատվական դաշտում:

1. Տեղեկատվական անվտանգությունը պետական մակարդակում

Հայաստանի կապի համակարգերը հիմնականում գտնվում են այլ պետություններին պատկանող ընկերությունների վերահսկողության տակ, որոնց գործունեությունը կարող է ապակառուցողական բնույթ ունենալ:

Այսպես, 2003թ. «ԱրմենՏել» ընկերությունը մեղադրվում էր Հայաստանի տարածքում բոլոր հեռախոսագանգերը լսելու մեջ: Կառավարության և հունական *OTE* ընկերության (այդ ժամանակ տնօրինում էր «ԱրմենՏելի» բաժնետոմսերի 90%-ը) միջև հերթական առճակատման ժամանակ «*WFI-consulting*» ընկերության փորձագետը, որին որպես վկա հրավիրել էր Հայաստանի կառավարությունը, հայտարարել է, որ «ԱրմենՏելի» թվային կայաններում ձայնագրվում են բոլոր հեռախոսագրույցները, որոնք այնուհետև մի քանի ամիս պահպանվում են: Ընդ որում՝ ընկերությունում, որը վերահսկում էր հունական կողմը, գաղտնալսում և գրանցում էին ոչ միայն բջջային և ֆիքսված կապի բոլոր հեռախոսագանգերը, այլև վարկային քարտերով արվող բոլոր գործողությունները, որոնք իրականացվում էին բանկոմատների և *POS*-տերմինալների միջոցով: Այն ժամանակ «ԱրմենՏելի» գլխավոր տնօրենի պաշտոնակատար Գեորգիոս Վասիլակիսը լրագրողներին հայտարարեց, որ իսկապես որոշակի ձայնագրություն կատարվում է, սակայն դա արվում է միջազգային նորմերին լիակատար համապատասխանությամբ: Նրա խոսքերով՝ դա արվում է, որպեսզի «համապատասխան մարմինները կարողանան իրականացնել որոշակի աշխատանք» [1]: Հետագայում ընկերությունը հայտարարեց, որ խոսակցությունների ձայնագրությունն անհրաժեշտ է ընկերության բիլինգային համակարգի համար:

Փաստորեն, Հայաստանի քաղաքացիների (ներառյալ պետպաշտոնյաների) բոլոր բանակցությունները և ֆինանսական գործունեության մի մասը հայտնվել էին մի ընկերության վերահսկողության տակ, որը ներ-

կայացնում էր այլ պետություն:

2006թ. վերջին «ԱրմենՏել» ընկերությունը վաճառվեց ռուսական «Վիմպելկոմ» ընկերությանը: 2007թ. մարտի 24-ին Հայաստանի կառավարությունը որոշում ընդունեց «ԱրմենՏելի» իր 10% բաժնետոմսերը «Վիմպելկոմին» վաճառելու մասին [2]: Դրանով իսկ պետությունն օտարերկրյա ընկերության լիակատար տնօրինությանը հանձնեց ֆիքսված ամբողջ հեռախոսային ցանցը և բջջային կապի մի մասը: Բջջային կապի մյուս մասը պատկանում է K-Տելեկոմ ընկերությանը, որը «ՂարաբաղՏելեկոմի» դուստր ընկերությունն է, որի հետևում նույնպես կանգնած է օտարերկրյա լիբանանյան կապիտալը:

Վերջին տարիների մեկ այլ խնդիր է միջազգային ինտերնետ կապի «ԱրմենՏելի» մենիշխանությունը: Մի կողմից՝ չի բացառվում, որ ինչպես և հեռախոսակապի պարագայում՝ հունական ընկերությունը «հետևում» էր նաև Հայաստանից դուրս եկող ինտերնետ հոսքին, բնականաբար նաև՝ էլեկտրոնային նամակներին: Մյուս կողմից՝ մենատիրության պայմաններում «ԱրմենՏելը» չէր զարգացնում ինտերնետ կապը, ինչի հետ կապված էլ Հայաստանը կախված է միակ՝ Վրաստանի տարածքով անցնող օպտիկամանրաթելային մալուխից և պահուստային արբանյակային թույլ կապուղուց: Մալուխի բազմակի վնասվածքներն ամբողջ Հայաստանը գրեթե լիովին զրկում էին արտաքին աշխարհի հետ ինտերնետ կապից, ինչն անթույլատրելի է արդի իրողություններում:

Բացի այդ, ինտերնետ կապի թույլ զարգացածությունը հանգեցնում է նրան, որ հայկական սերվերներում զետեղված հայկական կայքերը դժվարահասանելի են այլ երկրներում: Այս ուղղությամբ հուսադրող փաստ է այն, որ «ԱրմենՏել» ընկերությունն աստիճանաբար զրկվում է ինտերնետ կապի մենատիրական իրավունքից. գործընթացը կավարտվի 2007թ. նոյեմբերին:

Որոշակի խնդիրներ կան նաև ծրագրային ապահովման բնագավառում, որից օգտվում են պետական կառույցները: Այսպես, 2007թ. հունվարի 30-ին Էդինբուրգում (Շոտլանդիա) ստորագրվեց համաձայնագիր Հայաստանի կառավարության և *Microsoft* կորպորացիայի համագործակցության մասին, որի համապատասխան՝ ընկերությունը Հայաստանում իրականացնելու է ներդրումային, կրթական և նորարարական ծրագրերի շարք [3]: Հայաստանի կառավարությունը աջակցում է *Windows XP* օպերացիոն համակարգի տեղայնացմանը (հայերեն թարգմանելուն): Այժմ շարունակվում են *Windows Vista-ի Office 2007* ծրագրերի փաթեթի տեղայնացման աշխատանքները [4]: Նման նախաձեռնությունը կարելի է համարել և փոխշահավետ, սակայն զուգահեռ պետք է հաշվի առնել հետևյալ իրողությունները:

Ընկերությունը չի թաքցնում իր էքսպանսիոնիստական մտադրու-

թյունները: *Microsoft*-ի բիզնես-կառավարման և ռազմավարության գծով տնօրեն Փոլ Մաքլեսթոնի խոսքերով՝ կորպորացիան ծրագրում է ընդլայնել իր գործունեությունը Հայաստանում: Մաքլեսթոնը տեղեկացրել է, որ մինչև 2010թ. կորպորացիան կպատրաստի բուհերի շուրջ 1000 շրջանավարտներ *Microsoft*-ի վկայականներով: «Կորպորացիայի այս նպատակը պայմանավորված է հայկական ձեռնարկություններում և պետապարատում կադրերի աճող պահանջարկով», - ասել է Փոլ Մաքլեսթոնը [5]: Այսպիսով, ընկերությունը մտադիր է Հայաստանի տեղեկատվական տեխնոլոգիաների ոլորտը կախվածության մեջ դնել իր ծրագրային արտադրանքից:

Չուտ տնտեսական տեսակետից *Microsoft* ընկերությունից թանկարժեք ծրագրային ապահովում գնելու և ներդնելու հսկայական ծախսերը որոշակի խնդիրներ են առաջացնում: Անգամ հարուստ Եվրոպայում նման քաղաքականությունը համարվում է տնտեսապես չհիմնավորված:

Սակայն առկա են նաև այլ խնդիրներ՝ կապված տեղեկատվական անվտանգության հարցերի հետ: Հայտնի է, որ *Microsoft* ընկերության արտադրանքը բավական խոցելի տեղեր ունի, որոնք կարող են առաջացնել ինչպես համակարգերի խափանումներ, այնպես էլ հանգեցնել հարձակումների ինչպես երկրի ներսում, այնպես էլ դրսում այսպես կոչված թշնամաբար տրամադրված օգտվողների կողմից: Այսպես, *SANS* ինստիտուտի և ԱՄՆ ենթակառուցվածքի պաշտպանության ազգային կենտրոնի (*NIPC*) կազմած «Ինտերնետում հարձակման ենթարկվող քսան թիրախներ»-ի ամենամյա վարկանիշով *Microsoft* ընկերության ծրագրային ապահովումը անվտանգության առաջատարն է մնում՝ տարեցտարի գրավելով վերին դիրքեր ամենախոցելի համակարգերի շարքում [6]:

Հատուկ ուշադրություն պետք է դարձվի նաև մամուլում մշտապես հայտնվող տեղեկատվությանը ԱՄՆ հատուկ ծառայությունների (մասնավորապես՝ տեղեկատվական հետախուզության համար պատասխանատու Ազգային անվտանգության գործակալության (*National Security Agency*) հետ *Microsoft* ընկերության համագործակցության մասին: Ընկերությունը բազմիցս մեղադրվել է նրանում, որ *Windows* օպերացիոն համակարգի ներսում կան թաքնված միջոցներ, որոնք ամերիկյան հատուկ ծառայություններին հնարավորություն են տալիս չթույլատրված ձևով մուտք գործել օգտվողների համակարգիչներ: Ավելին, ԱԱԳ-ն պաշտոնապես հաղորդել է, որ օգնություն է ցուցաբերել *Microsoft Windows Vista* նոր օպերացիոն համակարգի անվտանգության մշակմանը [7]: Քանի որ *Microsoft* ընկերությունը չի բացում իր ծրագրային ապահովման ծածկագրերը (կոդ), ապա հնարավոր վտանգը, որ Հայաստանը կարող է հայտնվել օտարերկրյա պետությունից կախվածության մեջ, չպետք է անտեսվի:

Այս առնչությամբ նշենք, որ Եվրոպայում արդեն առկա է փակ ծածկագրով ծրագրային ապահովումը բաց աղբյուրներով (*OpenSource*) փոխարինելու գործընթաց. նման օպերացիոն համակարգեր են *Linux-ի* համակարգերը կամ *OpenOffice* փաթեթը, որոնք ի վիճակի են փոխարինել *Microsoft Office-ին*: Այսպես, 2007թ. հունվարի 16-ին Եվրահանձնաժողովը հանձնարարական հղեց Եվրամիության անդամ երկրներին՝ անցնել բաց ծրագրային ապահովման: Եվրահանձնաժողովի հովանու ներքո անցկացված ուսումնասիրությունների տվյալներով՝ ներկայումս բաց ծրագրային ապահովումը՝ *Linux-ի* օպերացիոն համակարգերի գլխավորությամբ, հասել է հուսալիության և անվտանգության այնպիսի աստիճանի, որ հնարավոր է դրա զանգվածային ներդրումը [8]:

OpenSource-ի անցնելու որոշումներն արդեն մի քանի տարի ընդունվում են Եվրամիության առանձին երկրներում: Եվրահանձնաժողովի տվյալներով՝ 2010թ. տեղեկատվական տեխնոլոգիաների ոլորտի բոլոր ծառայությունների 32%-ը Եվրամիության երկրներում կորվի բաց կոդերով ծրագրային ապահովման հիմքի վրա:

2. Որքանով է Հայաստանը պատրաստ արդի տեղեկատվական իրողություններին

Համաշխարհային տնտեսական ֆորումի (*World Economic Forum*) ամենամյա *The Global Information Technology Report 2006–2007* հաշվետվության տվյալներով՝ տեղեկատվական տեխնոլոգիաների զարգացմամբ Հայաստանը 96-րդն է աշխարհի հետազոտման ենթարկված 122 երկրների մեջ: Այս վարկանիշը կազմելիս հաշվի է առնվում ինչպես SS շուկայի զարգացման, այնպես էլ այլ ոլորտների (օրինակ՝ կրթության) վրա նրա ունեցած ազդեցության ու ներթափանցման մակարդակը, ինչպես նաև իշխանությունների՝ SS ներդրմանն ուղղված քաղաքականության հաջողությունը [9]: Թուրքիան այդ վարկանիշով 52-րդն է, Ադրբեջանը՝ 71-րդը, Վրաստանը՝ 93-րդը: Նշենք, որ անցյալ տարվա համեմատ Հայաստանն իջել է 10 կետով, ինչը վկայում է այն մասին, որ հանրապետությունը հետ է մնում համաշխարհային զարգացման տեմպերից:

Բջջային կապի նկատմամբ «ԱրմենՏելի» մենաշնորհի վերացումից հետո Հայաստանն այս ուղղությամբ զարգանալու լուրջ թոփք կատարեց: Այսօր բջջային հեռախոսակապից օգտվողների թիվը հասնում է 1 մլն-ի, ընդ որում՝ *Viva Cell* ընկերությունը վերահսկում է շուկայի շուրջ 60%-ը [10]: Եվ այս պահի դրությամբ միայն *Viva Cell-ն* է տրամադրում *GPRS* ծառայություն, որն ապահովում է ինտերնետ կապ բջջային հեռախոսների միջոցով: «ԱրմենՏելն» առայժմ միայն տրամադրում է *WAP* արդեն հնացած ծառայու-

թյունը, թեև կան տեղեկություններ, որ *GPRS* համակարգն արդեն թեստավորման փուլում է:

Չնայած տեղեկատվական տեխնոլոգիաների ոլորտը երկրում ակտիվորեն զարգանում է, այնուամենայնիվ, ընկերությունները բարձրորակ կադրերի պակաս ունեն և հաճախ ստիպված են լինում օգնել բուհերին մասնագետներ պատրաստելու նպատակով, ինչպես դա անում են *Synopsys* և *Lycos* ընկերությունները [11]:

Հանրակրթության ոլորտում դրությունն այս ուղղությամբ դեռևս բավարար չէ: Այսպես, 2005թ. արդյունքներով երկրում 864 դպրոցականների միջին հաշվով բաժին էր ընկնում 10 համակարգիչ: 1467 հանրակրթական դպրոցներում օգտագործվում էր ընդամենը 5531 համակարգիչ, ինտերնետին միացած էին 279 դպրոց: Մայրաքաղաքի 259 դպրոցներում տեղադրված են 1787 համակարգիչներ, 74 դպրոց միացած են ինտերնետին: Մարզերում ամենից շատ համակարգիչներ՝ 723 հատ, ունեն Շիրակի մարզի դպրոցները, ինտերնետին միացած են 176 դպրոցներից 38-ը: Ամենաքիչ թվով համակարգիչներ՝ 193 հատ, ունեն Վայոց ձորի դպրոցները, ինտերնետից օգտվելու հնարավորություն ունեն 51 դպրոցներից 8-ի աշակերտները [12]:

Բացի այդ, դպրոցական ծրագրերը և ինֆորմատիկայի ուսուցիչների պատրաստվածությունը չեն համապատասխանում արդի իրողություններին:

Ընդհանուր առմամբ, մի շարք պատճառներով, ինչպես, օրինակ, ՏՏ սարքավորումներ ներկրելիս սահմանին հարկվող ԱԱՀ-ն, ինտերնետ կապի թանկությունը, Հայաստանը զարգացածությամբ զգալիորեն հետ է մնում և՛ արևմտյան երկրներից, և՛ նախկին Խորհրդային Միության հանրապետություններից: Այսպես, *ITU (International Telecommunication Union)* 2006թ. հաշվետվության տվյալներով՝ Հայաստանում ինտերնետից օգտվում է բնակչության շուրջ 5%-ը, այն դեպքում, երբ աշխարհում այդ ցուցանիշի միջինը հասնում է 18,4%-ի [13]: Ադրբեջանում այդ ցուցանիշը հասնում է 8%-ի, Թուրքիայում՝ 21%-ի: *Internet World Stats-ի* տվյալներով՝ 2000-2007թթ. ընթացքում Հայաստանում ինտերնետից օգտվողների թվի աճը կազմել է ընդամենը 436,7%, այն դեպքում, երբ Վրաստանում այն հասել է 778%-ի, Ադրբեջանում՝ 5556,7%-ի [14]:

3. Ազդեցիվ քաղաքականությունն ընդդեմ Հայաստանի և հայության

Հայաստանի տեղեկատվական անվտանգության մեկ այլ կարևոր հարցը վերաբերում է այս դաշտում հանրապետության դեմ ուղղված թշնամական գործողություններին: Վերջին տարիներին Հայաստանի և մեր ժողովրդի նկատմամբ թշնամաբար տրամադրված երկրները և խմբերն ակտիվորեն

օգտագործում են արդի տեղեկատվական տեխնոլոգիաները ոչ բարեկամական գործողությունների համար:

Ադրբեջանական և թուրքական քարոզչությունն ակտիվորեն օգտագործում է ինտերնետ ռեսուրսները՝ իրենց շահերն առաջ մղելու, Հայաստանը և հայությունը վարկաբեկելու նպատակով: Հարևան պետություններն իրենց քարոզչության համար մարդկային և ֆինանսական լուրջ ռեսուրսներ են ծախսում, և ինտերնետի հայկական հատվածն այս դաշտում դժվարությամբ է հաղթահարում մրցակցությունը:

Եթե քարոզչական բնույթի հայկական կայքերը մեծ մասամբ ստեղծվում են անհատների և Սփյուռքի կազմակերպությունների ջանքերով, ապա Ադրբեջանում և Թուրքիայում այս ուղղությամբ ծրագրված աշխատանք է տարվում՝ պետական ռեսուրսների ներգրավմամբ: Այսպես, օրինակ, վերջին մի քանի տարիներին ծպտյալ, բայց ակնհայտորեն պետական աջակցությամբ դինամիկորեն զարգանում էր *Day.az* տեղեկատվական-վերլուծական պորտալը: Ռեսուրսը, որով ինչպես ռուսերեն, այնպես էլ անգլերեն լեզուներով հրապարակվում են նյութերը, պատկանում է Միլլի մեջլիսի միջազգային հարաբերությունների և միջխորհրդարանական կապերի մշտական հանձնաժողովի անդամ Անար Մամեդխանովին: Ընդ որում՝ *Day.az* պորտալը, որում զետեղվում են նորություններ ռուսերենով և անգլերենով, լուրջ տեղ է զբաղեցնում ինտերնետում: Նշենք, որ հաճախ հայկական մամուլն այս ռեսուրսն օգտագործում է որպես տեղեկատվության աղբյուր, մինչդեռ այդ գործակալությունն աշխատում է ապատեղեկատվություն տարածելու ուղղությամբ:

Ըստ զանազան վարկանիշային տվյալների՝ ամսական *Day.az* պորտալ են այցելում շուրջ 300 հազ. օգտվողներ, օրական՝ ավելի քան 10 հազար: Ինտերնետում հրապարակման մեջբերումների ցուցիչը հավասար է 2100-ի, ինչը, ըստ Յանդեքս համակարգի տվյալների, 41-րդ ցուցանիշն է ցանցում բոլոր ռուսալեզու տեղեկատվական գործակալությունների մեջ: Համեմատության համար նշենք, որ ամենաշատ այցելվող հայկական պորտալներից մեկի՝ *PanArmenian.net*-ին հղումների ցուցիչը հավասար է 850-ի, *Panorama.am* կայքինը՝ 300, *A1+* (*www.a1plus.am*)-ինը՝ ընդամենը 30: Հղումների նման բարձր ցուցիչն ամրապնդում է *Day.az*-ի դիրքերը որոնողական համակարգերում: Այսպես, Յանդեքս համակարգում «Հայաստան նորություններ» առանցքային բառերով որոնողական հարցման պարագայում *Day.az*-ը զբաղեցնում է երրորդ տեղը (առաջին տեղում էլ զուտ հայկական ռեսուրսը չէ. *РИА Новости* ռուսական գործակալության «*Новости-Армения*» նախագիծը):

Ինտերնետը ողողված է թուրքական ռեսուրսներով, որոնցում քարոզչություն է վարվում Հայոց ցեղասպանության ճանաչման դեմ, ընդ որում՝

տեղեկատվությունը տարածվում է բազմաթիվ լեզուներով: Այսպես, «Հայկական հարց» կայքը (<http://www.ermenisorunu.gen.tr/>) թուրքական տեսանկյունից է ներկայացնում մեծ քանակությամբ նյութեր թուրքերեն, անգլերեն, գերմաներեն և ֆրանսերեն լեզուներով: Կան կայքեր, որոնցում ներկայացվում են նյութեր հայերի կողմից թուրքերի և ադրբեջանցիների ջարդերի մասին, օրինակ՝ *Armenian Reality*-ն անգլերեն և ֆրանսերեն լեզուներով (<http://www.armenianreality.com/>):

Պաշտոնական Երևանի մոտեցումը հակաքարոզչական գործունեության վերաբերյալ հստակ ներկայացրել է Հայաստանի արտգործնախարար Վարդան Օսկանյանը: 2006թ. նոյեմբերի 7-ին ելույթ ունենալով Ազգային ժողովում՝ Վ.Օսկանյանը հայտարարեց, որ միջոցների անբավարարության պատճառով տարեցտարի դժվարանում է մրցակցությունը Թուրքիայի և Ադրբեջանի հետ այնպիսի հարցերի շուրջ սեփական դիրքորոշումը քարոզելու գործում, ինչպիսին են Լեռնային Ղարաբաղը կամ փոխհարաբերություններն Անկարայի հետ: Նրա խոսքերով՝ Ադրբեջանը և Թուրքիան տարեցտարի ավելացնում են Հայաստանի դեմ ուղղված քարոզչության համար տրամադրվող միջոցները: «Այս նպատակի համար նրանք դիմում են տարբեր ընկերությունների, ինչի վրա ծախսվում են միլիոնավոր դոլարներ», - ասել է նախարարը: Նշելով, որ Հայաստանը ներկայումս ի վիճակի չէ նման միջոցներ հատկացնել, Վարդան Օսկանյանն ընդգծել է օտարերկրյա կապիտալի ներգրավման անհրաժեշտության մասին [15]:

Սակայն փաստ է, որ կշռադատված քաղաքականության պարագայում ինտերնետում քարոզչություն վարելն այնպիսի լուրջ ֆինանսական ծախսեր չի պահանջում, որոնք Հայաստանը չկարողանա հոգալ: Մանավանդ եթե ներգրավվեն Միջուռքի և բազմաթիվ կամավորական խմբերի ռեսուրսները, որոնք առանց այդ էլ աշխատում են այդ ուղղությամբ: Սրանից հետևում է, որ մեր պետական կառույցները չունեն հակաքարոզչություն վարելու իրապես մշակված քաղաքականություն: Արդյունքում՝ Հայաստանի համար այնպիսի կարևոր կայքեր, որոնք նվիրված են ցեղասպանության հարցին (օրինակ՝ ռուսերեն *Genocide.ru*-ն), մշակվում և պահվում են մասնավոր նախաձեռնությունների հաշվին: (Բմիջիայրոց, նշենք, որ ադրբեջանական կողմը հակահայ քարոզչության նպատակով օգտագործում է նույնիսկ միջազգային կազմակերպությունների փողերը, ինչը սկզբունքորեն տեղի չպիտի ունենար, իսկ պաշտոնական Երևանը պետք է հետևեր և արձագանքեր նման անթույլատրելի իրողություններին: Այսպես, օրինակ, ադրբեջանական «Էլեկտրոնային գրադարանային ցանցը» (<http://kitab.az/>), ուր օն-լայն ռեժիմով զետեղված են մեծ քանակությամբ հակահայ հավակնոտ նյութեր, համաֆինանսավորվում է *IREX-IATP* կազմակերպու-

թյան կողմից, որը գործում է նաև Հայաստանում):

Բացի այդ, հիմնական արտաքին քաղաքական հարցերի առումով հայկական կողմը հետ է մնում տեղեկատվական ռեսուրսների զարգացածությամբ: Օրինակ՝ Ղարաբաղի հարցի հետ կապված՝ ադրբեջանական կողմն ինտերնետում ակտիվ քաղաքականություն է վարում՝ մեծ ծախսեր անելով: Հայկական ցանցային ռեսուրսները գրեթե ուշադրություն չեն դարձնում Լեռնային Ղարաբաղին, բացի այն հարցերից, որոնք կապված են բանակցային գործընթացի հետ: Վերջին ժամանակներս միայն սկսեցին աշխատել մի քանի դարաբաղյան ռեսուրսներ, որոնք փորձում են լուծել այդ խնդիրը: Դրանցից են *KarabakhOpen-ը* (<http://karabakhopen.com>), *Karabakh News-ը* (<http://www.karabakh-news.com>) և *Karabakh Live-ը* (<http://karabakhlive.com/>):

Սակայն ադրբեջանական կողմը շարունակում է պահել դիրքերը հայկական ռեսուրսների քաղաքականության պատճառով: Այսպես, ամենատարածված ռուսալեզու Յանդեքս որոնողական համակարգում «Ղարաբաղ» առանցքային բառով որոնում տալիս (տվյալները վերաբերում են 2007թ. ապրիլի սկզբին) վարկանիշով առաջին տեղում են ռուսական «Ռեզնում» գործակալության նյութերը: Երկրորդ տեղում է հայկական *Karabagh.am* էջը, որը թարմացվում էր 2002-ից: 6-րդ տեղում է հայկական *ArmenianHouse.org* գրադարանը: Մյուս բոլոր որոնողական հարցումների աղբյուրները ռուսական են: 10-րդ տեղում *Baku.ru* պորտալն է:

Ամենախոշոր որոնողական *Google* համակարգում «*Karabakh*» առանցքային բառով հարցման արդյունքներով առաջին տեղում է *Wikipedia* բաց հանրագիտարանի էջը (որը կարող է խմբագրել յուրաքանչյուր այցելու, ինչի հետ կապված՝ այդ էջի բովանդակությունը ժամանակի ընթացքում փոխվում է): Երկրորդ տեղում *Karabakh.org* կայքն է, որն ստեղծվել է ադրբեջանական տեսանկյունից Ղարաբաղյան հակամարտության լուսաբանման համար: Եվ նոր միայն երրորդ տեղում է ԼՂՀ ԱԳՆ կայքը, որը հեռու է կատարյալ լինելուց: Այնուհետև հաջորդում են մի քանի վերլուծական կայքեր, որոնք ստեղծվել և ուղղորդվում են տարբեր երկրներում ապրող ադրբեջանցիների կողմից, բրիտանական *BBC* հեռուստակայանի խիստ հավակնոտ էջը՝ նվիրված Ղարաբաղյան հարցին: Շարքը եզրափակում է ԼՂՀ կառավարության կայքը, որը գտնվում է 10-րդ տեղում:

Հաշվի առնելով այն փաստը, որ ըստ վիճակագրության՝ որոնողական համակարգերից օգտվողների մեծամասնությունը հարցման առաջին տասը արդյունքներից հետո դադարեցնում է որոնումը, ստացվում է այնպես, որ հայկական կողմը լրջորեն հետ է մնում ադրբեջանականից՝ Ղարաբաղյան հարցի շուրջ սեփական կարծիքը մատուցելու առումով: Այսպես, Փենսիլվանիայի համալսարանի հետազոտության տվյալներով՝ օգտվողների 54%-

ը նայում է որոնման արդյունքների առաջին էջը, 19%-ը՝ երկու և 10%-ից պակաս՝ նաև երրորդ էջը: Օգտվողների շուրջ 55%-ը որոնման արդյունքներից նայում է միայն առաջին կայքը: Որոնողական համակարգերից օգտվողների ավելի քան 80%-ը մեքենայի առաջարկած առաջին երեք հղումների արդյունքներից ավելին չի նայում [16]:

Տեղեկատվական անվտանգության նկատմամբ նման մոտեցումը հանգեցնում է նրան, որ հայկական մամուլի համար տեղեկատվության աղբյուր են դառնում թուրքական, ադրբեջանական կամ այլ ոչ բարեկամական ռեսուրսների մատուցած կասկածելի նյութերը: Ինտերնետի դերի աճի հետ մեկտեղ մեծանում է այլ պետությունների կողմից ապատեղեկատվության ներթափանցման չափը: Ընդ որում՝ հայկական մամուլում նկատվում է ապատեղեկատվության «ներմուծման» հնարավորությունների մասին հիմնական օրենքների չիմացությունը, որոնցով առաջնորդվում է այսօրվա ինտերնետը: Չկան լրագրողների և խմբագիրների բանիմացության բարձրացմանն ուղղված մեխանիզմներ, բացի այն միջոցառումներից, որոնք անցկացնում են միջազգային կազմակերպությունները տարբեր նախագծերի շրջանակներում, որոնք որևէ կապ չունեն Հայաստանի տեղեկատվական անվտանգության հետ:

Այսպես, փետրվարի 23-ին թուրքական ցանցային *Takvim.com.tr* ռեսուրսը տեղեկատվություն տարածեց այն մասին, որ ԱՄՆ 100 առաջատար գործարարներ, այդ թվում և Բիլ Գեյթսն ու Ուորեն Բաֆեթը, նամակ են հղել նախագահ Ջորջ Բուշին՝ հայերի ցեղասպանությունը չճանաչելու կոչով [17]: Նյութը ներկայացվել էր միայն թուրքերեն լեզվով: Այնուհետև *Turkish Daily News*-ը նյութը վերահրատարակել է անգլերեն լեզվով: Դրանից հետո ադրբեջանական ցանցային լրատվամիջոցներն ակտիվ շրջանառության մեջ դրեցին «նորությունը», ինչից հետո այն ներկայացրեց գրեթե ողջ հայկական մամուլը՝ առանց աղբյուրները ստուգելու: Բանը հասավ նրան, որ *Microsoft* ընկերության հայկական ներկայացուցչությունը հարկադրված էր հանդես գալ պաշտոնական հերքմամբ:

Միայն Հայաստանի Հանրապետության Ազգային անվտանգության ռազմավարությունում (այդ փաստաթուղթը 2007թ. փետրվարի 7-ին ստորագրվել է ՀՀ նախագահի կողմից) հռչակվեցին պետության տեղեկատվական անվտանգությանն առնչվող հիմնական կետերը: Սակայն փաստաթղթում տեղեկատվական բաղադրիչը բավարար չափով լուսաբանված չէ: Միայն որպես ներքին մարտահրավեր նշված է ենթակառուցվածքային ցանցի, այդ թվում՝ կապի համակարգերի զարգացման անբավարար մակարդակի մասին:

Հայաստանի Հանրապետության կարևոր հարցերի շարքում տեղե-

կատվության ոլորտին են վերաբերում երկու կետ.

- ինտեգրում միջազգային տեղեկատվական դաշտում, Հայաստանի և հայության մասին միջազգային հանրությունում իրական պատկերացումների ձևավորում պրոֆեսիոնալ մակարդակով, դիմակայություն ապատեղեկատվությանը և բացասական քարոզչությանը,
- ինտերնետ գլոբալ ցանցում Հայաստանին նվիրված հայերեն, ծավալով և որակով հավասարակշռված տեղեկատվության ապահովում՝ հայագիտության բոլոր ճյուղերի և հայության հետ կապված հարցերի վերաբերյալ:

Ցավոք, առայժմ ներկայացված կետերի իրականացման իրական մեխանիզմների մասին տեղեկատվություն չկա:

Նշենք նաև, որ նույնների վերջին որոշում է ընդունվել ՀԱՊԿ Անվտանգության խորհուրդների քարտուղարների կոմիտեին կից տեղեկատվական քաղաքականության և անվտանգության հարցերով ժամանակավոր աշխատանքային խումբ ստեղծելու մասին, ուր ընդգրկված է նաև Հայաստանը: Ենթադրվում է, որ ժամանակավոր աշխատանքային խմբի հիմնական խնդիրն է պատրաստել գործնական առաջարկություններ տեղեկատվական ոլորտի մարտահրավերներին ու սպառնալիքներին դիմակայելու համատեղ միջոցառումների համախմբման և ՀԱՊԿ անդամ պետությունների շահագրգիռ մարմինների միջև տեղեկատվության փոխանակման կատարելագործման վերաբերյալ [18]:

4. Հայերենի խնդիրները տեղեկատվական դաշտում

Եթե պետությունը նախաձեռնի ակտիվորեն աշխատել ինտերնետի հայերեն հատվածի զարգացման ուղղությամբ, դրան զուգահեռ հարկ կլինի լուծել տեխնիկական բազմաթիվ խնդիրներ: Այսպես, մեծ դժվարությամբ է լուծվում ինտերնետում հայերեն տեքստերի ընթերցման, հայկական հատվածի, որոնման համակարգերի ցուցակագրման խնդիրը և այլն: Բացի այդ, այնքան էլ պարզ չէ, թե խոսքն արդյոք միայն արևելահայերենին է վերաբերում, թե արևմտահայերենը նույնպես նկատի է առնվելու: Եթե պետությունն ուշադրությունը կենտրոնացնի միայն ինտերնետի արևելահայերեն հատվածի վրա, շահագրգիռ օգտվողների թվաքանակը բավական փոքր կլինի, և ծախսված միջոցների դիմաց ստացված արդյունքն էլ ցածր: Բացի այդ, հայության վերաբերյալ հարցերի լուսաբանումը կարևոր է նաև նրանց համար, ովքեր հայ չեն:

Փաստ է նաև այն, որ սփյուռքահայերի մի մասը բավականաչափ չի տիրապետում հայերենին: Հայաստանում ևս ինտերնետից օգտվող քաղա-

քացիների մեջ կան շատերը, ովքեր ռուսերենը կամ անգլերենը նախընտրում են հայերենից: Այս մասին կարելի է դատել անհատական ինտերնետի էջերի, ինտերնետ-օրագրերի (բլոգ), ֆորումների միջև առկա անհավասարակշռությունից, որոնցում հայերենը շատերի, նույնիսկ Հայաստանում ապրողների համար հիմնական լեզու չէ [19]:

Բացի այդ, ինտերնետում և ծրագրային ապահովման մեջ հայերենի կիրառումը մինչև օրս լուրջ խնդիր է ներկայացնում: Դեռևս վերջնականորեն չի լուծվել հայոց լեզվի ստանդարտի հարցը: Շատ օգտվողների համար, որոնք ծրագրային ապահովումից օգտվելու սահմանափակ գիտելիքներ ունեն, լուրջ խնդիր է հայերեն սայթերի ընթերցումը, հայերեն լեզվով էլեկտրոնային նամակներ գրել-կարդալը և այլն:

Չնայած նոր հայկական կայքերի մեծ մասը գրվում է *Unicode-ի* կիրառմամբ, որի «ճանաչումը» հեշտացվել է Հայաստանում ամենատարածված *Windows* օպերացիոն համակարգի նոր ձևերից օգտվողների համար, այնուամենայնիվ, մեծ քանակությամբ ինտերնետ ռեսուրսներ շարունակում են մնալ *ArmSCII* կոդավորման հիմքով, ինչը շատ օգտվողների համար անհնար է դարձնում էջերի ընթերցումը հայերեն լեզվով՝ առանց լրացուցիչ ջանքերի, որոշակի իմացության կամ լրացուցիչ ծրագրային ապահովման: Նշենք, որ նման կոդավորում օգտագործվում է նաև պաշտոնական կայքերի մեծ մասում, ինչպես, օրինակ, կառավարության (<http://www.gov.am/>), Ազգային ժողովի (<http://www.parliament.am/>), նախագահի (<http://www.president.am/>) կայքերում, մինչդեռ պաշտպանության նախարարության կայքը (<http://www.mil.am/>) հիմնված է *Unicode* կոդավորման վրա, ինչը վկայում է այն մասին, որ Հայաստանում դեռևս առկա է այս ոլորտում միասնականացման խնդիրը:

Լուրջ է նաև ազգային որոնողական համակարգի բացակայության խնդիրը, որն օգտվողներին հնարավորություն կտար ինտերնետում որոնում իրականացնել հայերեն կայքերում: *Google* որոնողական համակարգը հայերեն որոնման հնարավորություն տալիս է, սակայն այն հարմարեցված չէ հայերենի ձևաբանությանը և այդ առումով լիարժեք չէ: Ստանդարտ կոդավորման բացակայությունը նույնպես դժվարություն է նման ծրագրեր մշակողների համար, քանի որ ինտերնետի որոշակի հատված անջատվում է ինդեքսավորման գործընթացից:

Ճիշտ է, կային հայկական որոնողական համակարգերի ստեղծման մի քանի նախագծեր, ինչպես, օրինակ, *BanBer-ը* (արդեն չի գործում) կամ *HiFind-ը* (<http://www.hifind.am/>), բայց դրանք ի վիճակի չէին լուծել որոնողական համակարգերից ակնկալվող իրական խնդիրները: Եվ քանի որ հարցը լիարժեք լուծում չի ստանում, կայք կազմողների մի մասը հարկա-

դրված հրաժարվում է հայերեն լեզվից: Մյուս կողմից՝ հայերեն ռեսուրսները դուրս են մնում ինտերնետային իրական գործընթացներից այն պատճառով, որ օգտվողները որոնողական համակարգերում դրանցից անմիջականորեն օգտվելու հնարավորություն չունեն: Իսկ ինտերնետ-վիճակագրությունը ցույց է տալիս, որ հենց որոնողական համակարգերի միջոցով են հիմնականում օգտվողները մտնում կայքեր:

Ազգային որոնողական համակարգի ստեղծումը կենսական անհրաժեշտություն է, և այն լուրջ ֆինանսական ծախսեր է պահանջում: Սակայն հայկական ինտերնետային հատվածի փոքր չափերը հաշվի առնելով՝ դժվար է ենթադրել, որ այս ոլորտում ներդրումները կկատարվեն առևտրային կազմակերպությունների կողմից: Առավել հավանական է, որ ֆինանսավորումը կատարվի երկու աղբյուրի կողմից. միջազգային դոնորների կողմից (ինչպես դա եղավ *HiFind-ի* պարագայում, որի ստեղծման համար ֆինանսավորումը տրամադրել է Բաց հասարակություն ինստիտուտը 2004թ.) կամ պետության կողմից: Սակայն դոնորների դրամաշնորհների վրա հիմնված նախագծերը հաճախ, ինչպես ցույց է տալիս փորձը, կենսունակ չեն:

5. Ցանցային ընկերությունների դերի մասին

Այսօր ինտերնետում ավելի մեծ տարածում և ազդեցություն են ձեռք բերում ցանցային տարբեր ընկերություններ: Վերջին տարիներին առավել տարածված են դարձել ինտերնետ ֆորումները, որոնք բանավիճային ակումբներ են ներկայացնում: Առկա են ինչպես ընդհանուր, այնպես էլ մասնագիտացված ֆորումներ: Բացի այդ, ֆորումները շատ ակտիվ են մեծ սփյուռք ունեցող ժողովուրդների (ռուսներ, հրեաներ, հայեր, վրացիներ, ադրբեջանցիներ և այլն) մեջ:

Ադրբեջանցիները և թուրքերը ֆորումի հարթակներն օգտագործում են հայերին վարկաբեկելու համար: Բոլոր ֆորումներում, որոնցում քննարկվում են կարևոր թեմաներ, «ներկա» են ինտերնետից օգտվող ադրբեջանցիները և թուրքերը, որոնք փորձում են ներկայացնել իրենց տեսակետն այլ ժողովուրդների ներկայացուցիչներին: Ընդ որում՝ նրանք հաճախ գործում են միավորված՝ փոքր խմբերով: Գրեթե բոլոր ռեսուրսներում, որոնցում հրապարակվում են Հայաստանին, Ղարաբաղին և Ադրբեջանին առնչվող նյութեր, այդ խմբերի ներկայացուցիչները մասնակցում են: Նրանց գործունեությունը հաճախ ուղղորդվում է դրսից: Նրանք համառորեն աշխատում են տարակույսներ ունեցողների հետ, հմտորեն վարկաբեկում Հայաստանն ու Ղարաբաղը: Նրանց հիմնական նպատակն է ներկայացնել իրենց երկրի դիրքորոշումը, իրականացնել քարոզչություն, վարկաբեկել հակառակորդին:

Բացի հայ-ադրբեջանական և հայ-թուրքական հակամարտությունների վերաբերյալ իրենց պատկերացումներն ուղղակիորեն ներկայացնելուց, գործի են դրվում նաև անմաքուր մեթոդներ: Այսպես, ֆաշիստական աշխարհայացքին հակամետ ֆորումներում հայերը ներկայացվում են որպես սեմիթականներ, սիոնիստներ: Հրեական ֆորումներում ակտիվ քարոզչություն է վարվում հոգուտ այն բանի, որ հայերն արմատական հակասեմիթականության կողմնակիցներ են: Ակտիվ քննարկվում է նաև հայ-վրացական թեման՝ գործելով «ուրիշի դրոշի» ներքո: Ինտերնետ ֆորումներում ներգրավվածների մեծաթվությունից ելնելով՝ կարելի է ասել, որ ադրբեջանական և թուրքական քարոզչությունը որոշակի հաջողություններ ունի հակահայկական տրամադրությունների ձևավորման գործում [20]:

Այսօր արդեն ֆորումներն ակտիվությամբ իրենց տեղը զիջում են ինտերնետ-օրագրերին: Վերջին երկու տարիներին ինտերնետում դրանց թիվն անսահմանափակ աճել է: *Technorati-ի* տվյալներով, որը հետևում է ինտերնետ օրագրերի ոլորտին, 2007թ. ապրիլի սկզբի դրությամբ ինտերնետում 70 մլն օրագիր կա: Ընդ որում՝ օրը 120 հազ. կամ վայրկյանում 1,4 նոր օրագիր է ի հայտ գալիս [21]:

Այս ոլորտը նույնպես արդեն օգտագործվում է հակահայկական նպատակներով: Օրինակ՝ գործում է բացառապես հակահայկական ուղղվածություն ունեցող ադրբեջանա-թուրքական բլոգը (<http://azeri-turk.blogspot.com/>): Բլոգերն օգտագործում են նաև ռուս ազգայնականները հայերի դեմ հիստերիա հրահրելու համար: Այս ուղղությամբ հատկապես ակտիվ են աշխատում *Ընդդեմ անլեզալ ներգաղթի շարժման* ներկայացուցիչները: Այս կազմակերպության անդամներից մեկն իր բլոգում օգտագործել էր *OpenArmenia.com* ֆորումից վերցված տեքստի հատվածներ Մոսկվայում ֆաշիստների կողմից Վիզեն Աբրահամյանցի սպանությանը հայերի ռեակցիայի մասին, որպեսզի անշահավետ տեսանկյունից ներկայացվի հայկական սփյուռքը Ռուսաստանում [22, 23]: Դրանից հետո նրա «Խուճապ մետաղավանդակում» հաղորդագրությունը լայնորեն գովազդվեց (60-ից ավելի հղում)՝ ցանցային ընկերություններում հակահայկական ալիք առաջացնելով [24]:

Ինտերնետային ապատեղեկատվությունը կամ քարոզչական նյութերը տարածվում են ոչ միայն լրատվական, այլ նաև ցանցային ընկերությունների միջոցներով: Ադրբեջանական կամ թուրքական ՋԼՄ-ի կողմից ապատեղեկատվության «ներարկումից» հետո գործի են անցնում տեղեկատվական ճակատի մարտիկները: Ինտերնետից օգտվող ադրբեջանցիների հսկայական բանակն սկսում է տարածել այդ նյութերը հնարավոր բոլոր ֆորումներով, բլոգերով, ցանցային այլ միջոցներով: Նման քայլը կտրուկ ընդլայնում է «ներարկված» տեղեկատվության լսարանը՝ դրանով հանդերձ

մեծացնելով նաև որպես աղբյուր նշվող ադրբեջանական ՋԼՄ համբավը:

Թուրքերը և ադրբեջանցիներն սկսել են ակտիվորեն օգտագործել նաև նոր ինտերնետային հնարավորություն, այն է՝ տեսանյութերի տարածում այնպիսի ռեսուրսի միջոցով, ինչպիսին է *YouTube*-ը (www.youtube.com): Ինտերնետում զետեղվում են մեծ թվով տեսահոլովակներ, օրինակ, Խոջալուի դեպքերի մասին: Հաշվի առնելով այն, որ դաժանությունն ինտերնետում բավական մեծ «ժողովրդականություն է վայելում», նման նյութերն արագ տարածվելու միտում ունեն:

6. *Գրոհներ ինտերնետի հայկական հատվածի վրա*

Վերջին տարիներին հաճախակի են դարձել հայկական ռեսուրսների (ոչ միայն հայաստանյան, այլև Սփյուռքի հայերի կողմից պահվող) վրա հաքերային հարձակումներն ադրբեջանցիների և թուրքերի կողմից: Դրանց արդյունքում կայքերի աշխատանքը կամ ժամանակավորապես կանգ է առնում, կամ դրանք խափանվում են, կամ էլ հօգուտ իրենց է փոխվում դրանցում զետեղված տեղեկատվությունը:

Հայերի ու ադրբեջանցիների ինտերնետ-բախումները բավական հին պատմություն ունեն: Ընդունված է կարծել, որ պատմության մեջ ամենախոշոր ու առաջին ինտերնետ-պատերազմներից մեկը Հայաստանի և Ադրբեջանի հաքերային խմբերի բախումն է եղել, որոնց հետևում, կարելի է կռահել, կանգնած են եղել պետական կառույցները: 2000թ. հունվարին ադրբեջանական *Green Revenge* և *Hijack Team 187* հաքերային խմբերը կարողացան 3 օր իրենց վերահսկողության տակ վերցնել հայկական խոշոր պորտալների շուրջ 25 տիրույթ (դոմեն). պրովայդերներ, ՋԼՄ, Հայոց ցեղասպանության մասին կայքեր: Ի պատասխան՝ հայկական *Liazor group*-ը փետրվարին իր վերահսկողության տակ վերցրեց ինտերնետի գրեթե ողջ ադրբեջանական հատվածը: Ընդ որում՝ ադրբեջանական հեղինակավոր հրատարակություններից մեկի կայքում, վկայակոչելով պետական կառույցները, ապատեղեկատվություն զետեղվեց այն մասին, որ Ադրբեջանը պատրաստ է զիջումների գնալ Ղարաբաղյան հարցում: Ապատեղեկատվությունը կրկնեց հայկական «Մնարք» լրատվական գործակալությունը, որից հետո այն տարածվեց աշխարհով մեկ, ինչը մեծ արձագանք գտավ: Հայերի վերահսկողության տակ հայտնվեցին նաև ադրբեջանական դեսպանությունների, միջազգային կազմակերպությունների ներկայացուցչությունների և այլ կայքեր: Արդյունքում՝ Ադրբեջանի Ազգային անվտանգության նախարարությունն ստիպված էր հանդես գալ հայտարարությամբ, որ վերահսկում է ադրբեջանցի հաքերներին, ինչից հետո հայկական կողմը դադարեցրեց

«ռազմական գործողությունները» [25]:

Վերջին տարիներին հայկական ռեսուրսների վրա հարձակումների թիվը մեծանում է, չնայած այնպիսի գլոբալ բախում, ինչպիսին էր 2000 թվականինը, դեռ չի եղել: Հարվածների հաջորդ մեծ փոխանակումը տեղի ունեցավ 2005թ. գարնանը: Այդ ժամանակ հայկական ֆորումների վրա առաջին հարձակումները գրանցվեցին ադրբեջանցիների կողմից: Ոչնչացվեցին մի շարք ռեսուրսներ, ինչից հետո «մարտական գործողությունները» լայն թափ ստացան: Ոչնչացվեցին ինչպես մեկ, այնպես էլ մյուս կողմի տասնյակ վերկայքեր: Գրոհների զոհ դարձան հիմնականում բարձիթողիի մատնված, ինչպես նաև ոչ այնքան պրոֆեսիոնալ մակարդակով կառավարվող ինտերնետ-ֆորումները: Սակայն բավական երկար ժամանակով խափանվեց հայկական մի քանի խոշոր ցանցային ընկերությունների (*Hayastan.com, Yerevan.ru, OpenArmenia.com*) աշխատանքը: Միաժամանակ երկու կարևոր հայկական ռեսուրսների վրա կատարվեցին հարձակումներ թուրք հաքերների կողմից. շարքից դուրս եկան *Genocide.ru, ArmenianHouse.org* պատմական տվյալների խոշորագույն բազաները: Այս փուլն աչքի էր ընկնում ադրբեջանական և թուրքական հաքերային խմբերի սերտաճմամբ:

Այդուհետև կես տարվա մեջ մոտավորապես մեկ անգամ պարբերականությամբ շարունակվում էին հարձակումները հայկական ռեսուրսների վրա (չհաշված միանգամյա հարձակումները, որոնց պարբերականությունն ավելի մեծ է): 2006թ. մի քանի հարձակումներ կատարվեցին ինտերնետի հայկական հատվածի վրա: 2006թ. մարտին «կոտրեցին» մի շարք կայքեր, սակայն հաքերների հիմնական նպատակը Եվրատեսիլին մասնակցող Անդրեի կայքն էր: Հիշատակված կայքը «կոտրելուց» հետո դրանում (ինչպես նաև մի քանի այլ ռեսուրսներում) զետեղվեցին Խոջալուի զոհերի լուսանկարները: Ադրբեջանական հաքերների հարձակման արդյունքները, իմիջիայլոց, չհեռացվեցին մոտ երկու շաբաթվա ընթացքում, ինչը խոսում է այն մասին, որ Հայաստանում ցանցային գործընթացներին լրջորեն չեն հետևում, չնայած այն բանին, որ Անդրեի ելույթն ընկալվում էր որպես իմիջի խնդիր ամբողջ հանրապետության համար:

Կիրեռպատերազմի զոհ դարձան նույնիսկ հունգարական վեբ-ռեսուրսները: 2006թ. ապրիլի 13-ին Ռամիլ Սաֆարովի դատավճռի հրապարակումից հետո ադրբեջանցի հաքերները, ի նշան բողոքի, «կոտրեցին» ուղիղ 100 հունգարական կայք [26]: Նրանց միացան նաև թուրքական խմբերը՝ «կոտրելով» ևս մի քանի հունգարական ռեսուրսներ:

Եթե նախկինում հիմնականում խափանում էին ինտերնետ ֆորում-

ները և ոչ առևտրային բնույթի կայքերը, որոնց տերերը ֆինանսական հնարավորություններ չունեն անվտանգության հարցերին լուրջ ուշադրություն դարձնելու համար, ապա վերջին ժամանակներս հարձակման թիրախ են դառնում նաև ավելի լուրջ ռեսուրսներ: 2007թ. փետրվարի 26-ին, Խոջալուի դեպքերի տարելիցին, ադրբեջանցի հաքերները «կոտրեցին» 15 հայկական ռեսուրս, այդ թվում Դե-ֆակտո գործակալության (<http://defacto.am/>) և Հայաստանի Օմբուդսմենի (<http://ombuds.am/>) կայքերը:

Ինտերնետի հայկական հատվածի անվտանգության ապահովման հարցը դառնում է կենսականորեն կարևոր, քանի որ հարվածի տակ են ընկնում այնպիսի ռեսուրսներ, որոնք ցանցում ներկայացնում են Հայաստանը: Մակայն ներկա պահին հայկական ռեսուրսների անվտանգության հետ կապված իրավիճակը պետական կառույցների ուշադրությունից դուրս է գտնվում:

Ամփոփում

Այսպիսով, Հայաստանն այսօր կանգնած է բազմաթիվ խնդիրների առջև՝ կապված տեղեկատվական անվտանգության հետ: Այս համատեքստում պետությունն սկսում է արժևորել հնարավոր վտանգները: Մինևայն ժամանակ, տեխնիկական զարգացումն աշխարհում պահանջում է արագ և դինամիկ պատասխաններ արդիականության մարտահրավերներին: Համաշխարհային հանրության զարգացման վերջին տարիների փորձը ցույց է տալիս, որ տեղեկատվական ոլորտի հետ կապված աճի տեմպերով հանրապետությունը շարունակում է հետ մնալ գլոբալ գործընթացներից: Ընդ որում՝ հետ է մնում ոչ միայն բարձր, այլև միջին զարգացած երկրներից:

Ստեղծված իրավիճակում Հայաստանը պետք է ունենա տեղեկատվական անվտանգության հետ կապված խնդիրների լուծման հստակ և գործուն ծրագիր, այլապես հետ կմնա արագ զարգացող գլոբալ իրողություններից: Այս պարագայում սպառնալիքի տակ կհայտնվեն ոչ միայն երկրի տնտեսական ու սոցիալական զարգացման, այլև ազգային անվտանգության հետ կապված հարցերը:

Ապրիլ, 2007թ.

Աղբյուրներ և գրականություն

1. Росбалт, 3 сентября 2003г.
2. PanARMENIAN.Net, 24 марта 2007г.
3. Новости-Армения, 10 апреля, 2007г.
4. Арминфо, 23.03.2007г.
5. Арминфо, 2007-04-10.
6. <http://www.sans.org/top20/>.
7. «Компьютерра», 1 февраля 2007г.
8. Economic impact of open source software on innovation and the competitiveness of the Information and Communication Technologies (ICT) sector in the EU, Prepared on November 20, 2006.
9. <http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm>
10. Данные компаний АрменТел и Viva Cell.
11. Հարցազրույց UITE ղեկավար Շարեն Վարդանյանի հետ, <http://internet.media.am/?i=361>
12. «Новости-Армения», 06/ 07/ 2006.
13. International Telecommunication Union, Measuring the Information Society, ICT Opportunity Index and World Telecommunication/ICT Indicators 2007.
14. <http://www.internetworldstats.com/stats3.htm>
15. ИА REGNUM, 7 ноября 2006г.
16. <http://www.psu.edu/ur/2003/websiteappeal.html>
17. <http://takvim.com.tr/2007/02/23/akt101.html>
18. Сообщение пресс-службы Секретариата ОДКБ, 09/12/2006.
19. Հակոբյան (Թարմուշյան) Ռ., Հայաստան հայերենը՝ Համացանցում: Ռազմավարության և անվտանգության հարցեր: Երևան, 2007:
20. Мартиросян С., «Кибер-война за Карабах», Росбалт, 19.05.2006, <http://www.rosbalt.ru/2006/05/19/253927.html>
21. <http://technorati.com/weblog/2007/04/328.html>
22. ИТАР-ТАСС, 22 апреля, 2006.
23. <http://forum.openarmenia.com/index.php?showtopic=10448&st=0>
24. <http://doppel-herz.livejournal.com/172453.html>
25. Мартиросян С., «Цензура в интернете: Запад не отстает от Востока», CNews.Ru, http://www.cnews.ru/reviews/index.shtml?2006/02/16/196225_1
26. PanARMENIAN.Net, 07.03.2007.

НЕКОТОРЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ АРМЕНИЯ

Самвел Мартиросян

Резюме

На нынешнем этапе мирового развития все большую значимость обретает проблема информационной безопасности, а для находящейся в кольце транспортной блокады Армении значение информационных технологий и вовсе трудно переоценить. Важным аспектом информационной безопасности нашей страны и армянства в целом являются агрессивные действия враждебно настроенных государств и социальных групп. Последние в своей пропаганде используют новейшие технологии. Армения и армянский народ лицом к лицу столкнулись с серьезной информационной войной, которую развязали сопредельные государства. Возможные механизмы противостояния – еще один аспект информационной безопасности.