

Տեղեկատվական անվտանգություն սցենարների մշակում, իրականացում և հետադարձ կապ

Տեղեկատվական անվտանգությանը վերաբերող խնդիրները լուրջ մարտահրավեր են ողջ աշխարհում: Ժամանակից աշխարհում վիրտուալ իրականություն են տեղափոխել հասարակության ու պետության կենսագործունեության գրեթե բոլոր ոլորտները՝ ռազմաքաղաքական, սոցիալ-տնտեսական, մշակութային: Ընդ ուրում, ինտերնետի համընդհանուր հասանելիության պայմաններում յուրաքանչյուր ոք հանդիսանում է ոչ միայն ինֆորմացիայի սպառող ու կրող, այլև ունի անսահմանափակ մեղիա կոնտենտ արտադրելու և տարածելու հնարավորություն:

Հայաստանի պարագայում տեղեկատվական անվտանգությանը վերաբերող խնդիրներն օրակարգային են առաջին հերթին աշխարհաքաղաքական իրողությունից ելնելով: Որևէ մեկի համար գաղտնիք չէ, որ գրեթե ամեն օր ստիպված ենք դիմակայել հակառակորդ պետությունների կողմից իրականացվող քարոզչությանը, որը հսկայական մարդկային և նյութական ռեսուրսներ է պահանջում: Համացանցի սրընթաց զարգացումը և ՁԼՄ-ների թվի աճն էլ իրենց հերթին խիստ բարդացրել են տեղեկատվական անվտանգությանը ապահովման գործընթացը՝ դարձնելով այն ազգային անվտանգություն կարևորագույն բաղադրիչ:

Հայաստանի Հանրապետության տեղեկատվական անվտանգության խնդիրները տեսականորեն կարելի է բաժանել երկու մասի՝ տեխնիկական, որն ընդունված է կոչել «կիրեռ անվտանգություն» և բովանդակային, որը վերաբերում է քարոզչական, հակաքարոզչական, զանգվածային լրագրության, տեղեկատվական հոսքերի հետ առնչվող խնդիրներին:

Կարող եմ փաստել, որ տեխնիկական ապահովման առումով լուրջ հաջողությունների ենք հասել. պետական ռեսուրսները կիրեռ հանցագործություններից պաշտպանության բարձր մակարդակ ունեն: Իսկ մասնավոր սեկտորի պարագայում ունենք խնդիր: Պարբերաբար մասնագետներից տեղեկություն է ստացվում այս կամ այն մասնավոր ռեսուրսի դեմ հարձակման մասին, ինչը համագործակցության ոչ բավարար մակարդակի մասին է վկայում: Այս իմաստով կարևորում եմ այդ համագործակցության, ինչպես նաև հասարակության իրազեկվածության մակարդակի բարձրացմանն ուղղված համապատասխան գործողությունների կազմակերպման անհրաժեշտությունը:

Բովանդակայինի մասով խնդիրն ավելի բարդ է, քանի որ նույնանման իրավիճակներ գրեթե չեն լինում և պետք է ամեն պահ, ամեն ինչի պատրաստ լինել: Այդուհանդերձ, արդյունավետ ռազմավարության մշակման համար անհրաժեշտ է տեսլականների, կանխատեսումների և գործողությունների սցենարների

պլանավորում: Այդ սցենարների իրագործումից հետո էլ պետք է հետադարձ կապով արդյունքների վերլուծություն իրականացնել, ինչը նոր ու ավելի արդյունավետ ռազմավարության մշակման հիմք կհանդիսանա:

Տեղեկատվական անվտանգության ապահովման տեսանկյունից մենք ունենք խնդիր թե՛ դրսում, թե՛ ներսում: Հայաստանը տասնյակ տարիներ ստիպված է դիմակայել Ադրբեջանի քարոզչական հարձակումներին ու, թեև, դաշտը զգալիորեն մաքրվել է, բայց այսօր էլ մենք բախվում ենք իրավիճակների, երբ հայկական ռեսուրսները՝ որոշ դեպքում հեղինակավոր, ադրբեջանական քարոզչական նյութեր են վերահրապարակում ու ինտենսիվորեն տարածում սոցիալական ցանցերում: Իսկ շարքային ընթերցողը չի էլ հասկանում, որ իրեն «քարոզչական խայծ է» հրամցվել: Պարտավոր էլ չէ: Բազմիցս խոսվել է այդ մասին, բայց ժամանակն է գործնական լուրջ քայլեր ձեռնարկել այդ ուղղությամբ: Ժամանակն է զբաղվել ոլորտի մասնագետների կրթական ցենզի բարձրացմամբ, ինչի կարիք այսօր շատ է զգացվում:

Միևնույն ժամանակ, ես շատ ուրախ եմ, որ Հայաստանում կան շատ լավ մասնագետներ տեղեկատվական անվտանգության որոտում, հատկապես տեղեկատվական տեխնոլոգիաների, կապի միջոցների, ինչպես նաև բովանդակային նյութերի մատուցման, բայց այս ամենը համակարգման կարիք ունի:

Իրականում համակարգման խնդիրը մեզ համար մեծ մարտահրավերներ է բոլոր ոլորտներում: Ունենք հայեցակարգեր, մշակած օրենքներ, կանոնակարգումներ, բայց համակարգը այդպես էլ լավ արդյունք չի տալիս: Արդյունքների հիման վրա դասեր քաղելը, հետադարձ կապով սցենարների փոփոխություն, կամ նորերի նախօրոք մշակումը մեր կառավարման համակարգում և կյանքում բացակայում է: Հենց այստեղ է, որ պետք է կարողանանք նոր մշակույթ ներմուծել, որպեսզի դիմակայենք մարտահրավերներին: Եվ այս ամենը հարկավոր է անել միջազգային փորձի ուսումնասիրության արդյունքում:

Արտաքին դաշտում քարոզչությանը դիմակայելու գործը թեև լուրջ նյութական ռեսուրսներ է պահանջում, բայց մենք ունենք հսկայական ներուժ փոքր ռեսուրսով մեծ խնդիրներ լուծելու համար: Այդ առումով պարզապես պետք է մոբիլիզացնել ռեսուրսները՝ թե՛ Սփյուռքում, թե՛ Հայաստանում: Այստեղ ևս համախմբման և հետևողական համակարգման անհրաժեշտություն կա: Վստահաբար ասում եմ, Հայաստանի ու Արցախի մասին միջազգային ճանաչում ունեցող լրատվամիջոցի մի հրապարկումն անգամ կարող է ի չիք դարձնել մի շարք նախազծեր, որոնց վրա մեր հակառակորդները միլիոնավոր դոլարներ են ծախսում:

Միևնույն ժամանակ, շատ կարևոր է հասկանալ, թե արտաքին աշխարհը, միջազգային հանրությունն ինչպե՞ս են ընկալում ու գնահատում իրողությունները: Մեր երկրի շահերին հակասող որևէ տեղեկատվություն սովորաբար որակում ենք «հակահայ»: Ես հասկանում եմ, որ մեր պատկերացմամբ դրանք հակահայ են, բայց

մեկ հարց՝ «Բացի մեզանից էլ ո՞վ է այդպես ընկալում»: Չէ, որ մեր շահերից չբխող տեղեկատվություն տարածող կողմն էլ ունի իր սեփականը: Կարծում եմ՝ քարոզչությանը դիմակայելու, բացասական ինֆորմացիոն ֆոնը չեզոքացնելու համար անհրաժեշտ է հստակ գնահատել՝ արտաքին աշխարհն ինչպե՞ս է ընկալում մեր կողմից «հակահայկական քարոզչություն» որակվողը:

Պետք է նկատի ունենանք, որ մյուս ազգերն ունեն իրենց սեփական ընկալումները և դրանք կարող են համահունչ չլինել մեր ընկալումներին: Եթե չառաջնորդվենք այս գործելաոճով, կպարփակվենք մեր ներքին իրողությունում ու կդադարեք աշխարհի հետ «նույն լեզվով խոսել», կամ որ ավելի վատ է՝ մեր գործողությունները կասկածանքով ու վերապահումներ կընդունվեն արտաքին լսարանի կողմից:

Ամփոփելով ելույթս՝ նշեմ, որ այսօր Հայաստանի Հանրապետության համար առաջին հերթին առանցքային նշանակություն ունի տեղեկատվական անվտանգության հայեցակարգի արդիականացումը՝ առկա մարտահրավերներին դիմակայելու և համակարգված քաղաքականություն իրականացնելու համար: Այն պետք է ոչ թե դարակներում փտող հերթական ձևական փաստաթուղթը լինի, այլ առօրյա գործածության աշխատանքային գործիք դառնա:

Եվ շատ կարևոր է, որ հայեցակարգի արդիականացում իրականացվի միջազգային համագործակցության պայմաններում՝ աշխարհի փորձը յուրացնելու ու տեղայնացնելու միջոցով: Հուսով եմ՝ տեղեկատվական անվտանգության ոլորում Հայաստանի գրանցած հաջողությունների մասին առաջիկայում միջազգային հարթակներում խոսելու առիթներ կլինեն, դրա համար մենք ունենք բավարար ռեսուրսներ՝ թե մարդկային, թե տեխնիկական, պարզապես կամք ու ջանքեր են անհրաժեշտ:

Շնորհակալություն: