# ՀԱՅԱՍՏԱՆ

## Թվային սպառնալիքների լանդշաֆտ. քաղաքացիական հասարակություն և լրատվամիջոցներ

Internews
Local voices. Global change.

CyberHUB

# Բովանդակություն

# Ընդհանուր տեղեկություններ

Նախորդ տարվա ընթացքում Հայաստանի մի քանի քաղաքական գործիչների և քաղաքացիական հասարակության կազմակերպությունների թիրախավորման համար օգտագործվել է Pegasus լրտեսական ծրագիրը: Փորձագետները կապեր են գտել Pegasus-ի ներգրավմամբ այս միջադեպերի և Ադրբեջանի իշխանությունների միջև, ինչը միջազգային հակամարտության համատեքստում այս լրտեսական ծրագրի կիրառման առաջին դեպքն է: Հայաստանի և Ադրբեջանի միջև տարածքային վեճը առանցքային դեր է խաղում երկու երկրների կառավարման համար և մի շարք պատերազմների պատճառ է հանդիսացել: Թեև Հայաստանի կիբերսպառնալիքների լանդշաֆտը ներկայացնելիս ԶԼՄ-ները կենտրոնանում են հիմնականում լրտեսական ծրագրերի վրա, քաղաքացիական հասարակության կազմակերպությունները բազմաթիվ այլ թվային սպառնալիքների են բախվում:

Այս զեկույցը պատրաստել է Ինտերնյուսի՝ Համացանցի ազատության և դիմակայունության թիմը՝ մի գործունեության շրջանակում, որը սպառնալիքների վերլուծության և միջադեպերի արձագանքման տեղայնացված փորձագիտական գիտելիքի միջոցով հզորացնում է քաղաքացիական հասարակության կազմակերպությունների (ՔՀԿ-ների), լրագրողների և այլ իրավապաշտպանների (ԻՊ-ների)՝ թվային հարձակումները հայտնաբերելու, վերլուծելու և դրանց դիմակայելու ունակությունը: Այս զեկույցում ամփոփ ներկայացված են Հայաստանի քաղաքացիական հասարակության և լրագրողների առջև ծառացած սպառնալիքները, ինչպես նաև խորհուրդներ՝ թվային անվտանգության փորձագետներին, որոնք աջակցում են այս համայնքին: Զեկույցը նաև ընդհանուր տեղեկություններ է տրամադրում կիբերանվտանգության ոլորտին, որը, հնարավոր է, անհրաժեշտություն ունենա վերլուծելու Հայաստանի քաղհասարակության և լրագրողների վրա ազդող անվտանգության միջադեպերը: Զեկույցի ամփոփիչ մասում քննարկվում են մեղմման այն միջոցառումները, որոնք թվային անվտանգության փորձագետները կարող են առաջարկել այն կազմակերպություններին, համայնքներին և անհատներին, որոնց հետ աշխատում են:

Այս զեկույցը պատրաստվել է CyberHub-AM-ի՝ համակարգչային արտակարգ իրավիճակների արձագանքման թիմի (անգլ.՝ Computer Emergency Response Team, CERT) հետ սերտ համագործակցությամբ՝ Հայաստանի քաղհասարակության համար՝ ներառյալ ՀԿ-ներ, իրավապաշտպաններ, ակտիվիստներ, լրագրողներ և անկախ լրատվամիջոցներ: Հիշյալ թիմը գործում է իբրև կոնտակտային և աջակցման կենտրոն հայաստանյան վերոնշյալ խմբերի համար՝ հարկ եղած դեպքում հավաքելով, վերլուծելով և անանուն ու պատասխանատու կերպով միջադեպերի տվյալները և ցուցիչները տրամադրելով սպառնալիքների համաշխարհային հետախուզական համայնքին:

Այս զեկույցում մատնանշված սպառնալիքները, միտումները և պրակտիկ օրինակները վեր են հանվել ռիսկային խմբերին թվային անվտանգության անմիջական աջակցության (որը տրամադրել են Ինտերնյուսը և CyberHub-AM-ը), գրասենյակային հետազոտության և Համացանցի ազատության (անգլ.՝ Internet Freedom) համայնքի վստահելի անդամների հետ զրույցների միջոցով: Այս զեկույցը մեկտեղում է միջադեպերի արձագանքման աշխատանքների տվյալները՝ արձանագրելով Հայաստանին բնորոշ հարձակման օրինաչափությունները:

*Հոկտեմբեր 2023*

*Հեղինակներ և խմբագիրներ՝ Մարտին Գրուտեն, Էշլի Ֆաուլեր, Մարկ Շաֆեր և Սքայլեր Սալիկ*
*Սրբագրումը, ձևավորումը և էջադրումը՝ Սքայլեր Սալիկի*

# Թվային սպառնալիքների լանդշաֆտը

## Քաղաքական համատեքստը, քաղաքացիական հասարակությունը և լրատվամիջոցները

ԽՍՀՄ-ից անկախանալուց հետո Հայաստանը շարունակական հակամարտության մեջ է Ադրբեջանի հետ, որը հանգեցրել է բազմաթիվ զինված բախումների: Հակամարտության հիմքում մի տարածք է, որը հայերն անվանում են Արցախ, իսկ միջազգային հանրությունը՝ Լեռնային Ղարաբաղ: Ադրբեջանը վերջերս ներխուժեց Լեռնային Ղարաբաղի տարածք, ինչը հանգեցրեց տեղի էթնիկ հայ բնակչության զանգվածային արտագաղթի:[1]

*2023 թվականի սեպտեմբերին Ադրբեջանը լայնածավալ ներխուժում սկսեց Լեռնային Ղարաբաղ, և 24 ժամվա ընթացքում տեղի հայկական ուժերը հանձնեցին վերահսկողությունը: Այս ռազմական գործողությունից հետո ավելի քան 100,000 էթնիկ հայեր լքեցին տարածաշրջանը, ինչը մարդասիրական խոշոր ճգնաժամի պատճառ դարձավ:*

Լեռնային Ղարաբաղի առաջին պատերազմը տեղի է ունեցել 1988-1994 թվականներին՝ մինչև Ռուսաստանի միջնորդությամբ հրադադարի հաստատումը: Այդ համաձայնագրով Հայաստանը վերահսկում էր Լեռնային Ղարաբաղի տարածքի մեծ մասը, իսկ շարունակվող լարվածությունը դիտարկվում էր տնտեսական խնդիրների առանցքային պատճառ ինչպես Հայաստանում, այնպես էլ Ադրբեջանում: 2020 թվականին Լեռնային Ղարաբաղի համար ևս մեկ լայնածավալ պատերազմ բռնկվեց, որը տևեց վեց շաբաթ՝ մինչև պատերազմող կողմերի՝ նոր զինադադարի համաձայնվելը: Շատ հայեր, սակայն, այս զինադադարը, համարում են պարտություն:

2023 թվականի հոկտեմբերին՝ այս զեկույցի պատրաստմանը զուգահեռ, Հայաստանում իրավիճակն արագորեն փոխվում էր: 2023 թվականի սեպտեմբերին Ադրբեջանը լայնածավալ ներխուժում սկսեց Լեռնային Ղարաբաղ, և 24 ժամվա ընթացքում տեղի հայկական ուժերը հանձնեցին վերահսկողությունը: Այս ռազմական գործողությունից հետո ավելի քան 100,000 էթնիկ հայեր լքեցին տարածաշրջանը, ինչը մարդասիրական խոշոր ճգնաժամի պատճառ դարձավ:[2] Գրելու պահին շատերը մտավախություն ունեին, որ Ադրբեջանը կշարունակի իր ագրեսիան՝ ներխուժելով արդեն նաև Հայաստանի հարավ: Ադրբեջանի կառավարությունը, սակայն, հերքում է նման էսկալացիայի հնարավորությունը: Ադրբեջանը Հայաստանին կոչ է արել խաղաղ ճանապարհով միջանցք ստեղծել, որը թույլ կտա կապվել Ադրբեջանի Նախիջևան էքսկլավին: Նախկինում Ադրբեջանը սպառնացել էր ուժով բացել այդ միջանցքը: Ներխուժման պատճառով ԱՄՆ Պետդեպարտամենտը 2002 թվականից ի վեր առաջին անգամ չի երկարաձգել «Ազատության աջակցության ակտի» (անգլ.՝ Freedom Support Act) կասեցումը, որը թույլ է տալիս զենք վաճառել Ադրբեջանին:[3]

Եվրոպայի հետ ամուր հարաբերություններին զուգահեռ՝ Հայաստանը սերտորեն կապված է նաև Ռուսաստանի հետ: Ռուսերենը ամենատարածված օտար լեզուն է, և ռուսները վիզայի կարիք չունեն Հայաստան այցելելու համար: Ռուսաստանը նաև ռազմաբազա ունի Հայաստանում. Ռուսաստանի 102-րդ ռազմակայանը տեղակայված է Գյումրիում և գտնվում է

ՌԴ զինված ուժերի Հարավային ռազմական օկրուգի հրամանատարության ներքո: Ռուսաստանը խաղաղապահ ուժեր ունի նաև հայ-ադրբեջանական սահմանին և Լեռնային Ղարաբաղում, թեև այդ ուժը զգալիորեն կրճատվել է Ուկրաինա լայնամասշտաբ ռազմական ներխուժման պատճառով: Այդ ներխուժումից հետո շատ ռուս SS և տեխնոլոգիական աշխատողներ, ինչպես նաև Ռուսաստանի քաղաքացիական հասարակության որոշ ներկայացուցիչներ և լրագրողներ տեղափոխվել են Հայաստան:[4] 2022 թվականին Հայաստանը ձեռնպահ է քվեարկել ՄԱԿ-ի բանաձևին, որը պահանջում էր Ռուսաստանից դադարեցնել ռազմական գործողությունները և դուրս գալ Ուկրաինայի տարածքից:[5]

Ադրբեջանի՝ Լեռնային Ղարաբաղ ներխուժումից հետո Ռուսաստանի չմիջամտելը անորոշություն է առաջացրել ռուս-հայկական հարաբերությունների ապագայի շուրջ: Դրան գումարած՝ Հայաստանը հավելյալ աջակցություն չի ստացել Հավաքական անվտանգության պայմանագրի կազմակերպությանն (ՀԱՊԿ) իր անդամակցությունից, ինչն այդ անդամակցության արդյունավետության հետ կապված հարցեր է առաջացրել: 2023 թվականի հոկտեմբերին Հայաստանը վավերացրեց Հռոմի ստատուտը՝ այդպիսով միանալով Միջազգային քրեական դատարանին: Այժմ որպես ՄՔԴ անդամ՝ Հայաստանի իշխանությունները պարտավոր են ձերբակալել ՌԴ նախագահ Վլադիմիր Պուտինին վերջինիս՝ Հայաստան մուտք գործելու դեպքում: Ռուսաստանը վճռականորեն դեմ է արտահայտվել այս քայլին:[6]

Հայաստանի քաղաքացիական հասարակությունը և լրատվամիջոցները հիմնականում ազատորեն գործելու հնարավորություն ունեն: Այնուամենայնիվ, վերջին տարիներին սահմանափակումների աճ է գրանցվել, և տարածաշրջանային զարգացումներին զուգահեռ իրավիճակը կարող է փոխվել: Հատկանշական է քաղհասարակության ունեցած ակտիվ դերակատարումը 2018 թվականի բողոքի ցույցերին, որոնք հանգեցրին իշխանափոխության:[7] 2021 թվականին Հայաստանի կառավարությունը սկսեց կիրառել զրպարտության մասին օրենքներ, որոնք օգտագործվում էին լրագրողներին պատասխանատվության ենթարկելու համար: Այնուամենայնիվ, ներքին և միջազգային դիմադրությամբ պայմանավորված՝ դրանք չեղարկվեցին 2022 թվականին:[8] Ըստ «Լրագրողներ առանց սահմանների» (անգլ.՝ Reporters Without Borders) կազմակերպության՝ Հայաստանի կառավարությունը բավարար չափով չի պաշտպանում մամուլի ազատությունը. նշվում է, որ լրագրողների նկատմամբ բռնությունները հաճախ անպատիժ են մնում:[9]

Խոսքի ազատության և քաղհասարակության կազմակերպությունների ազատ գործունեության դեմ սպառնալիքներն ընդհանուր առմամբ ավելի հաճախ են հանդիպում՝ վնասելով առանց այն էլ խոցելի խմբերին: Բավականին վերջերս տեղի ունեցած քրեական հետապնդման մի դեպք ակնառու է դարձնում խոսքի ազատության և քաղաքացիական հասարակության սպառնալիքները. խտրականության կենտրոնում է հայտնվել եզդի էթնիկ փոքրամասնությունը, որն առավելապես միատարր երկրում ամենամեծ էթնիկ խումբն է: Իշխանությունները ձերբակալել են Հայաստանում Մարդու իրավունքների եզդիական կենտրոնի ղեկավար Սաշիկ Սուլթանյանին՝ փոքրամասնությունների իրավունքների պաշտպանությանն ուղղված իր գործունեությամբ ատելություն և բռնություն հրահրելու մեղադրանքով:[10] Հայաստանը չունի խտրականության դեմ հատուկ օրենք, և ոլորտն ուսումնասիրողները մտավախություն ունեն,

որ այս դեպքն ավելի լայն իմաստով կաշկանդող ազդեցություն կունենա խոսքի ազատության վրա:[11]

***Խոսքի ազատության և քաղհասարակության կազմակերպությունների ազատ գործունեության դեմ սպառնալիքներն ընդհանուր առմամբ ավելի հաճախ են հանդիպում՝ վնասելով առանց այն էլ խոցելի խմբերին:***

Հայաստանի ԼԳԲՏՔ+ համայնքը նույնպես բախվում է համատարած խտրականության ողջ երկրով մեկ, ինչն ազդում է ՔՀԿ-ների աշխատանքի արդյունավետության վրա:[12] Քուիր համայնքի շահերը ներկայացնող կազմակերպությունները, ինչպիսիք են «ՓԻՆՔ Արմենիան» և «Իրավունքի կողմ» ՀԿ-ն, բախվել են ահաբեկումների, սպառնալիքների մի դատական համակարգի պայմաններում, որը չի արձագանքում հոմոֆոբ բռնությանը:[13] Չնայած այս սպառնալիքներին, ԼԳԲՏՔ+ իրավապաշտպան կազմակերպությունները շարունակում են հանուն փոփոխությունների պայքարը՝ համագործակցելով ԶԼՄ-ների և կառավարության հետ, ինչպես նաև աջակցություն տրամադրելով հայաստանցի քուիր անձանց:[14]

## Կիբերանվտանգությունը Հայաստանում

Հայաստանն առաջին անգամ համացանցին միացել է 1994 թվականին՝ .am վերին մակարդակի դոմեյնի ներդրմամբ: Այդուհանդերձ, միայն մոտավորապես 2010-ին համացանցի օգտագործումը երկրում համատարած բնույթ ստացավ:[15] Ռուսաստանի հետ Հայաստանի սերտ հարաբերությունները հավանաբար նպաստել են երկրում ֆինանսական նպատակներ հետապնդող հաքերների ազատ գործելուն: 2013-ին ըստ Verizon-ի՝ Հայաստանը, հատկապես նրա չափսերը նկատի առնելով, մեծ թվով նման չարագործների է «հյուրընկալել»:[16] 2012-ին խոշոր սպամ ուղարկող «Bredolab» բոտնետի ենթադրյալ հեղինակը՝ հայկական ծագմամբ մի ռուսաստանցի, չորս տարվա ազատազրկման է դատապարտվել Հայաստանի իշխանությունների կողմից:[17]

Ըստ Հայաստանի ոստիկանության տվյալների՝ 2016-2018 թվականներին կիբերհանցագործությունների 20-25% աճի միտում է արձանագրվել: Երկրում կիբերհանցագործության հիմնական տեսակը թիրախից ֆինանսական ռեսուրսների հափշտակումն է. դրա ամենատարածված եղանակներն են բանկային գործարքները և բանկային քարտերից գումարի հափշտակումը: Հարձակում գործողները բանկային տվյալները հափշտակելու նպատակով սոցիալական ցանցերի միջոցով թիրախավորում են քաղաքացիներին՝ հաճախ նրանց որևէ հարազատի նմանակելով:[18] 2019 թվականին հայերից և հնդիկներից բաղկացած կազմակերպված հանցավոր խմբավորումը տեխնիկական աջակցության խոշոր խարդախություն է իրականացրել՝ թիրախավորելով ԱՄՆ-ի և Կանադայի օգտատերերի:[19]

Հանրահայտ Telegram և WhatsApp մեսենջեր հավելվածների հայաստանյան օգտատերերը հաճախ խարդախությունների և հաքերային հարձակման փորձերի թիրախ են դառնում: Համաձայն CyberHub-AM-ի տրամադրած տեղեկությունների՝ չարամիտ մղումներով

հաղորդագրությունները հաճախ գրվում են ռուսերեն, և որոշ օգտատերեր կարող են Ռուսաստանի քաղաքացիներին թիրախավորող արշավների անուղղակի զոհ դառնալ:

Քանի որ Telegram-ը և WhatsApp-ը կապված են օգտատիրոջ հեռախոսահամարին, յուրաքանչյուր ոք, ով ունակ է միջամտություն ունենալու SMS հաղորդագրությանը, կարող է տիրանալ օգտահաշվին, եթե առկա չէ լրացուցիչ պաշտպանություն իրականացնող գաղտնաբառ: Չնայած թիրախավորող սոցիալական ինժեներիայի կիրառմամբ դեպքերին՝ օգտահաշիվներին տիրանալը սովորաբար իրականացվում է առանց հստակ շարժառիթի: Բացի այդ, շատ մարդիկ, որոնք չեն օգտվում WhatsApp-ից, հայտնում են, որ իրենց հեռախոսահամարներն օգտագործվել են WhatsApp-ի օգտահաշիվ ստեղծելու համար: Այս փաստը թույլ է տալիս ենթադրել, որ հարձակում գործողները մուտք ունեն կա՛մ հեռահաղորդակցական ընկերություն, որն ստանում է օգտահաշվի նույնականացման SMS հաղորդագրությունները, կա՛մ այն հարթակներ, որոնք օգտագործվում են դրանք ուղարկելու համար:

Վերջին տարիներին Հայաստանում արձանագրվել են պետության կողմից հովանավորվող թվային հարձակումների դեպքեր: 2019-ին Ռուսաստանի հետ առնչություն ունեցող Turla խումբը «ջրարբ» (անգլ.՝ watering hole) տեսակի հարձակման[i] միջոցով կոտրեց հայկական չորս կարևոր կայքեր, որոնցից երկուսը պատկանում էին կառավարությանը. սա արձանագրել է կիբերանվտանգության ESET ընկերությունը:[20] Խմբավորման նախկին գործունեությունից և կոտրած կայքերից դատելով՝ Turla-ն հավանաբար ցանկանում էր հարձակումն իրականացնելիս թիրախավորել քաղաքական գործիչների և պետական պաշտոնյաների:

2021 թվականին լրտեսական ծրագրերի արտադրությամբ զբաղվող իսրայելական Candiru ընկերության ծրագրով թիրախավորվել են նաև հայաստանցիներ՝ իբրև լայնամասշտաբ արշավի մաս: Հարձակումների հիմքում Microsoft-ի[21] ծրագրային ապահովման՝ զրոյական օրվա խոցելիություններն էին:[ii] Այս արշավի թիրախում էին հայտնվել քաղաքական գործիչներ, իրավապաշտպաններ և լրագրողներ: Մոտավորապես նույն ժամանակ Google-ը հայտարարեց, որ Հայաստանում թիրախները ստացել են Google Chrome-ի՝ զրոյական օրվա խոցելիությունները օգտագործող հղումներով նամակներ:[22]

2022 թվականին հակառակորդի սպառնալիքների մասին զեկույցում Meta-ն հայտնել է վնասակար ծրագրերի (անգլ.՝ malware) և ֆիշինգի, ինչպես նաև կեղծ օգտահաշիվների և կայքերի կիրառմամբ ադրբեջանական գործողության մասին:[23] Թեև հարձակումն առավելապես ներադրբեջանական էր, այն ազդեցություն է ունեցել նաև Հայաստանում որոշ անհատների վրա:

[i] «Ջրարբ» (անգլ.՝ watering hole) տեսակի հարձակման ժամանակ հարձակում գործողները կոտրում և վնասակար ծրագրով վարակում են այն կայքը, որն ամենայն հավանականությամբ այցելում են թիրախավորված խմբի ներկայացուցիչները: Այդկերպ թիրախավորված հարձակումը տեղի է ունենում առանց ուղղակիորեն թիրախներին առնչվելու:

[ii] Զրոյական օրվա խոցելիությունները (անգլ.՝ zero-day vulnerabilities) այն խոցելիություններն են, որոնք կիրառման պահին անհայտ են մնում հարձակման զոհ դարձած ծրագրային ապահովում արտադրողին:

## Քաղհասարակության և լրատվամիջոցների կիբերանվտանգության վիճակը

Քաղաքացիական հասարակության կազմակերպությունները և լրատվամիջոցները նույն հարձակումներին են բախվում, ինչ Հայաստանում համացանցի բոլոր օգտատերերը, սակայն, իրենց աշխատանքի բնույթով պայմանավորված, նրանք առանձնահատուկ սպառնալիքների էլ են հանդիպում, իսկ ոչ թիրախավորված հարձակումները հաճախ ավելի մեծ ազդեցություն են գործում: Քաղհասարակության առանձին անդամի համար ոչ միշտ է պարզ՝ հարձակումը թիրախավորվա՞ծ էր, թե՞ ոչ: Նրանց Telegram-ի, WhatsApp-ի և սոցիալական մեդիայի այլ օգտահաշիվները հաճախ են վտանգվում, նրանց կայքերը կոտրվում են, դառնում DDoS հարձակումների թիրախ: Կայքը կոտրելու մի օրինակ, որն ազդել է ՔՀԿ-ի վրա, կարելի է տեսնել ստորև ներկայացված պրակտիկ օրինակում:

> ***Քաղհասարակության առանձին անդամի համար ոչ միշտ է պարզ՝ հարձակումը թիրախավորվա՞ծ էր, թե՞ ոչ: Նրանց Telegram-ի, WhatsApp-ի և սոցիալական մեդիայի այլ օգտահաշիվները հաճախ են վտանգվում, նրանց կայքերը կոտրվում են, դառնում DDoS հարձակումների թիրախ:***

Ինչպես ամբողջ աշխարհում, այնպես էլ Հայաստանում բազմաթիվ լրատվամիջոցներ և քաղաքացիական հասարակության այլ խմբեր գործում են սահմանափակ ռեսուրսներով: Նրանց թվային անվտանգության վրա պարբերաբար ազդում են իրենց իսկ կայացրած որոշումները: Դրանցից են՝ հնացած ծրագրերի գործարկումը կամ կոտրած, չլիցենզավորված ծրագրերի ներբեռնումը համացանցից՝ պաշտոնական տարբերակը գնելու փոխարեն: Վերջին երևույթն այնքան տարածված է, որ հայտնի են դեպքեր, երբ կազմակերպությունները, ունենալով պաշտոնական լիցենզավորված ծրագիր, այդուհանդերձ ներբեռնել են կոտրած տարբերակը:[24]

Մի կազմակերպություն, որն աշխատում էր կոտրած ծրագրով, թվային հարձակման էր ենթարկվել. այդ ծրագրի օգտագործումը ցանցում keylogger տեղադրելու հնարավորություն էր տվել՝ իր հերթին նպաստելով, որ չարագործները տիրանան կազմակերպության Google-ի օգտահաշվին: Ցանցում վնասակար ծրագրի առկայության մասին Google-ի նախազգուշացումից հետո միայն սպառնալիքը հայտնաբերվեց:

Մեկ այլ ՀԿ մի քանի հազար ԱՄՆ դոլար է կորցրել կորպորատիվ էլ-նամակների վրա հարձակման (անգլ.՝ business email compromise, BEC) հետևանքով, որի միջոցով կոտրվել է կազմակերպության Yahoo-ի օգտահաշիվը: Հաքերները, օգտագործելով օգտահաշիվը և սոցիալական ինժեներիայի հնարքները, իրենց արդեն իսկ հասանելի էլեկտրոնային հասցեից նամակ են ուղարկել դոնորին՝ համոզելով գումար ուղարկել հարձակում գործողների ստեղծած բանկային հաշվին: Չնայած այս խարդախությունն իր մասշտաբով զիջում է BEC-ի կիրառմամբ այլ դեպքերին, սակայն ՀԿ-ն շատ է տուժել հարձակումից:[25]

Այդ սպառնալիքներից շատերի դեպքում կարելի է գտնել Ադրբեջանի հետ կապ ունեցող խմբերի հետքը: Օրինակ՝ 2022 թվականի հոկտեմբերին ադրբեջանցի հաքերները տիրացել էին հնացած և խոցելի ծրագրային ապահովմամբ աշխատող հայկական մի հոսթինգ պրովայդերի: Սա հանգեցրել էր նրա վրա գործող բոլոր կայքերը կոտրելուն: Թեև հարձակումն ուղղակի հասցեատեր չուներ հաճախորդների շրջանում, կայքերից երկուսը պատկանում էին տեղական հասարակական կազմակերպությունների:[26] Թուրքական խմբերը ևս պարբերաբար թիրախավորել են հայկական կայքերը:

> ***Ադրբեջանի իշխանությունները ձեռք են բերել Pegasus-ը և օգտագործել այդ լրտեսական ծրագիրը՝ թիրախավորելու տեղացի ակտիվիստներին և լրագրողներին՝ ցուցադրելով միաժամանակ ծրագիրը Հայաստանում աշխատեցնելու իրենց կարողությունը:***

Ի լրումն թվային անվտանգության թույլ հիգիենայի պատճառով և սոցիալական ինժեներիայի կիրառմամբ տեխնիկապես քիչ բարդ հարձակումների, որոնք ազդում են ողջ երկրի վրա, որոշ հայտնի հայեր, այդ թվում քաղաքացիական հասարակության անդամներ և լրագրողներ, թիրախ են դարձել նաև երկու տեսակի նորագույն լրտեսական ծրագրերի՝ Predator-ի և Pegasus-ի:

2021 թվականի դեկտեմբերին Meta-ն[27] և Citizen Lab-ը[28] միասին առաջին անգամ հայտնեցին Հյուսիսային Մակեդոնիայում գտնվող Cytrox ընկերության մշակած Predator լրտեսական ծրագրի մասին: Նշվում էր, որ Cytrox-ի որոշ հաճախորդներ գտնվում են Հայաստանում: Այդ ժամանակից ի վեր CyberHub-AM-ը հաստատել է «հայաստանյան քաղաքական և մեդիա թիրախներին» պատկանող մի քանի սարքերում Predator-ով վարակվածության դեպքերը, ինչը թույլ է տալիս կասկածել, որ այդ հարձակումների հետևում կանգնած են տեղական անվտանգության ծառայությունները:[29]

Հատկանշական է, որ Telegram-ի կոտրված օգտահաշիվներն օգտագործվել են Predator-ի տեղադրումն ապահովող հղումները տարածելու համար: Այս մարտավարությունը կարող է բացատրել վերը նշված առավել թիրախային օգտահաշիվների առևանգման որոշ դեպքեր: Սա խելացի հնարք է. ցածրից մինչև միջին ռիսկայնության անձանց օգտահաշիվներին սովորաբար ավելի հեշտ է տիրանալ, բարձր ռիսկայնության անձինք, իրենց հերթին, այդ հաշիվներից հաղորդագրությունները (չգիտակցելով, որ դրանք կոտրված են) վստահելի կհամարեն և ամենայն հավանականությամբ կսեղմեն հղումը:

Pegasus լրտեսական ծրագիրը, որը մշակել և վաճառում է Իսրայելում գործող NSO Group-ը, իր տեսակի մեջ «ամենահայտնին» է. այն բազմաթիվ լրատվական նյութերի, փոդքասթների և նույնիսկ գրքի թեմա է դարձել: Մեքսիկայում և ԱՄՆ-ում 2016 թվականին հայտնաբերված Pegasus-ի՝ Հայաստանում օգտագործման առաջին ապացույցներն ի հայտ եկան 2021-ի նոյեմբերին: Այդ ժամանակ Apple-ը ծանուցումներ տարածեց այն մասին, որ ազգային պետությունները գործողություն են իրականացնում iPhone-ի որոշակի քանակի օգտատերերի դեմ: Թեև սկզբնական շրջանում մեղադրանքներ էին հնչում Հայաստանի իշխանությունների հասցեին, փաստերը ցույց տվեցին, որ Հայաստանում Pegasus-ի կիրառման հետևում կանգնած են Ադրբեջանի իշխանությունները:[30]

2023 թվականին CyberHub-AM-ը միջազգային գործընկերների հետ միասին Լեռնային Ղարաբաղի երկրորդ պատերազմի ժամանակ Pegasus-ի օգտագործման դեպք բացահայտեց, ինչն էլ ավելի ուժեղացրեց այն կասկածները, որ դա Ադրբեջանի ձեռքի գործն է:[31] Ադրբեջանի իշխանությունները ձեռք են բերել Pegasus-ը և օգտագործել այդ լրտեսական ծրագիրը՝ թիրախավորելու տեղացի ակտիվիստներին և լրագրողներին՝[32] ցուցադրելով միաժամանակ ծրագիրը Հայաստանում աշխատեցնելու իրենց կարողությունը: Հայաստանցի մի կին լրագրողի դեմ Pegasus-ի օգտագործման դեպքի ուսումնասիրությունը տե՛ս պրակտիկ օրինակների բաժնում:

## Մեղմման միջոցառումներ

Օգտահաշվի անվտանգությունը կարևոր է Հայաստանում յուրաքանչյուրի և հատկապես քաղհասարակության և լրատվամիջոցների ներկայացուցիչների համար: **Երկփուլային վավերացման համակարգը (անգլ.՝ two-factor authentication) պարտադիր է**. այն մեղմում է թույլ և/կամ կրկնվող գաղտնաբառերի օգտագործման հետ կապված խոցելիությունները: Թեև երկրորդ փուլի առկայությունն ամեն դեպքում ավելի լավ է, քան դրա բացակայությունը, կան բազմաթիվ փաստեր, որ SMS-ի միջոցով վավերացումը Հայաստանում բավականաչափ անվտանգ չէ, հատկապես ռիսկային օգտատերերի համար: Որպես օրինակ՝ տե՛ս CyberHub-AM-ի հայերեն այս նյութը: Վավերացման հավելվածի օգտագործումն ավելի լավ է, քան SMS-ը, իսկ ընդհանրապես լավագույն անվտանգությունն ապահովում է կողերի գեներատոր սարքի (անգլ.՝ hardware token) օգտագործումը:

Որոշ մեսենջերներ, ինչպիսիք են Telegram-ը, WhatsApp-ը և Signal-ը, հաշվի ակտիվացման համար հեռախոսահամար են պահանջում: Երկփուլային վավերացման ակտիվացումը ներառում է **հավելյալ գաղտնաբառ**՝ ի լրումն հաշիվ մուտք գործելու համար ստացվող SMS հաղորդագրության. այդպիսով ապահովվում է անվտանգությունն այն դեպքերի համար, երբ որևէ մեկը ապօրինի հասանելիություն ստանա SMS-ներին: Երբ այս գործառույթն ակտիվացված է, հավելվածը պարբերաբար կխնդրի օգտատիրոջը մուտքագրել իր գաղտնաբառը՝ երաշխավորելով, որ հաղորդագրությունները հասանելի չեն որևէ մեկին, բացի օգտահաշվի սեփականատիրոջից: Սա կանխում է SMS-ները ճանկելու միջոցով օգտահաշիվներին տիրանալը, ինչը տարածված երևույթ է երկրում:

**Այնպիսի սարքերը, ինչպիսիք են նոութբուքները և բջջային հեռախոսները, պետք է պարբերաբար թարմացվեն**. անհրաժեշտ է օպերացիոն համակարգերում և այլ ծրագրերում կիրառել անվտանգության շտկումները այն պահին, երբ դրանք հասանելի են դառնում: **Ծրագրերը պետք է ձեռք բերվեն միայն պաշտոնական աղբյուրներից**, ինչը շատ դեպքերում վճար է պահանջում: ՀԿ-ները չպետք է կաշկանդվեն քննարկելու այդ հարցը դոնորների հետ կամ փնտրելու անվճար այլընտրանքներ. դա կարող են լինել կա՛մ բաց կոդով ծրագրակազմեր, կա՛մ ծրագրեր, որոնք անվճար կամ ավելի էժան տրամադրում են ծրագրակազմը իրավասու ՀԿ-ներին:

Ադրբեջանցի, ավելի հազվադեպ՝ նաև թուրք հաքերները սովորաբար թիրախավորում են հայկական ՀԿ-ների և քաղհասարակության կազմակերպությունների կայքերը DDoS և

բովանդակության աղավաղման (անգլ.՝ defacement) հարձակումներով: Եթե նման հարձակումից կազմակերպության տուժելու հավանականություն կա, նրանք պետք է կանխարգելիչ միջոցներ ձեռնարկեն, օրինակ՝ իրենց կայքի համար **օգտվելով DDoS-ի մեղմման այնպիսի ծառայություններից**, ինչպիսիք են Cloudflare-ը կամ Project Shield-ը: **Բովանդակության կառավարման համակարգը (որի վրա աշխատում է կայքը) և դրա խրվակները (անգլ.՝ plugin) մշտապես թարմացված վիճակում պահելուց զատ**, նրանց անհրաժեշտ է **ընտրել հոսթինգի այնպիսի պրովայդեր,** որն իր համակարգերում **հետևողականորեն կիրառում է անվտանգության շտկումներ**:

Կայքերի և այնպիսի սարքերի համար, ինչպիսիք են նոութբուքները և բջջային հեռախոսները, **կանոնավոր կրկնօրինակումը (անգլ.՝ backup)** թույլ է տալիս օգտատերերին վերականգնել տվյալները դրանց ջնջվելու կամ այն դեպքերում, երբ անհրաժեշտ է հետ բերել նախկին վիճակը: Հոսթինգ պրովայդերները կամ սարք արտադրողները երբեմն ավտոմատ կերպով ներդնում են կրկնօրինակման գործառույթը, ինչն ամենահարմար տարբերակն է: Եթե դա տեղի չունի, **ապա լավագույն լուծումը շաբաթվա կամ առնվազն ամսվա կտրվածքով նոր կրկնօրինակներ ստեղծելն է, համոզվելը, որ դրանք աշխատում են և ապահով պահեստավորելը**՝ կանխելով հենց դրանց թիրախ դառնալու վտանգը:

Առաջատար լրտեսական ծրագրերը, ինչպիսիք են Pegasus-ը և Predator-ը, սովորաբար օգտագործում են զրոյական օրվա խոցելիությունները և հատկապես առաջինի դեպքում՝ օգտատիրոջ կողմից զրոյական միջամտությամբ վարակումները (անգլ.՝ zero-click infections): Սա ենթադրում է, որ բոլոր հնարավոր թարմացումներն ունեցող սարքը կարող է վարակվել այնպես, որ օգտատիրոջը չի հաջողվի դրա դեմն առնել՝ ընդունված կանխարգելիչ միջոցառումներ կիրառելով, օրինակ՝ խուսափելով կասկածելի հղումների կամ հավելվածների վրա սեղմելուց: Լրտեսական ծրագրերով վարակվելու վտանգի տակ գտնվողները պետք է հաշի առնեն սա:

Պոտենցիալ թիրախներին խորհուրդ է տրվում հաղորդագրությունների փոխանակման հավելվածներում օգտագործել **դրանց անհետացող տեսակները**, երբ հաղորդագրությունը ավտոմատ կերպով ջնջվում է նշված ժամանակից անմիջապես հետո: Սա կարող է նվազեցնել ապագայում օգտահաշիվը կոտրելու հետևանքով պատճառված վնասը: Տարանջատումը (անգլ.՝ compartmentalization)՝ **աշխատանքի և անձնական օգտագործման առանձին սարքերի կիրառումը** (իսկ **բարձր ռիսկայնությամբ աշխատանքի համար ևս մեկ առանձին սարքի կիրառումը**) նույնպես նվազեցնում է վնասի չափը, բայց դա ակնհայտորեն լրացուցիչ ծախսեր և անհարմարություններ է առաջացնում:

Հեռախոսները թարմացված վիճակում պահելուց բացի, **iPhone-ների կանոնավոր վերագործարկումը** (կարելի է օրական մեկ անգամ) և **Apple-ի կողպման ռեժիմի օգտագործումը** նույնպես մեղմում են հարձակումները:

Շատ ավելի քիչ է հայտնի Android համակարգը թիրախավորող լրտեսական ծրագրերի մասին, թեև դա չի նշանակում, որ Android օգտագործողների ռիսկերն ավելի փոքր են: Հայտնի է, որ ավելի թանկարժեք Android սարքերն ավելի անվտանգ են և սովորաբար նրանց ավելի արագ են հասանելի դառնում խոցելիություններից պաշտպանող շտկումները: Հավանականություն կա, որ

սարքի կանոնավոր վերագործարկումը նույնպես կմեղմի վնասը, քանի որ լրտեսական ծրագրերը վերագործարկումից հետո չեն պահպանվում:[iii] Թեպետ Android-ի դեպքում պետք է գիտակցել, որ դա կարող է նաև հեռացնել նախորդ վարակի ապացույցները: Որոշ օգտատերերի համար սա կարող է մտահոգիչ լինել:

# Պրակտիկ օրինակներ

## Կայքը կոտրելու դեպք WordPress-ի խոցելի խրվակի միջոցով

2023 թվականի մայիսին Հայաստանում փոքրամասնությունների իրավունքների պաշտպանությամբ զբաղվող մի կազմակերպության կայքը կոտրվեց, որի պատճառով կայքից օգտվողներն ուղղորդվում էին դեպի այնպիսի կայքեր, որոնք ակնհայտորեն խաբեությամբ էին զբաղվում, և որոնց բովանդակությունը կապ չուներ սկզբնական կայքի հետ: Քանի որ կազմակերպությունը պատրաստվում էր կարևոր զեկույց հրապարակել, նրանք «զգում էին», որ կայքը թիրախավորված է կոտրվել:

Միջադեպը հետաքննելու համար կազմակերպությունը դիմեց CyberHub-AM-ին՝ համակարգչային արտակարգ իրավիճակների արձագանքման թիմին (անգլ.՝ Computer Emergency Response Team, CERT): CyberHub-AM-ը աջակցում է Հայաստանի քաղհասարակությանը, ներառյալ՝ ՀԿ-ներին, իրավապաշտպաններին, ակտիվիստներին, լրագրողներին և անկախ լրատվամիջոցներին:

Տուժած կազմակերպության վեբկայքն աշխատում է բաց կոդով բովանդակության կառավարման հանրահայտ WordPress համակարգով, որը սովորաբար օգտագործում են ՀԿ-ները և քաղհասարակության կազմակերպությունները ողջ աշխարհում: Չարագործները հաճախ կարողանում են գտնել և օգտագործել WordPress-ի խոցելիությունները. մասնավորապես՝ այդ հարցում նրանց օգնում են բազմաթիվ խրվակները, որոնց միջոցով նրանք տիրանում են կայքերին՝ օգտագործելով դրանք չարամիտ նպատակներով կամ փոխելով դրանց բովանդակությունը, որը հայտնի է իբրև բովանդակության աղավաղում:

Հետաքննության ընթացքում CyberHub-AM-ը վեբ սերվերում որոնել է ոչ վաղ անցյալում փոփոխված ֆայլերը և հայտնաբերել վերջերս ավելացված կամ փոփոխված տարբեր ֆայլեր, որոնք պատկանում էին «posts-layouts» անվամբ խրվակին: Նրանք նաև նկատել են «de-mouser-44» նոր օգտատեր, որը որպես ադմինիստրատոր ավելացվել է WordPress-ի օգտահաշվին, ինչը հաստատում է, որ ինչ-որ արտաքին դերակատար մուտք է ունեցել հաշիվ:

[iii] Այդպես է iPhone-ի համար նախատեսված բոլոր հայտնի և հավանաբար նաև Android-ի համար նախատեսված այլ լրտեսական ծրագրերի դեպքում, հատկապես այն տեսակների, որոնք «արմատներ են գցում» սարքում:

CyberHub-AM-ը վերլուծեց այն հաջորդականությունը, որով շարժվում էին օգտատերերը կայք այցելելուց հետո և պարզեց, որ նրանց սկզբում ուղղորդում էին դեպի cdn[.]scriptsplatform[.]com: scriptsplatform[.]com դոմեյնն ընդամենը օրեր առաջ էր գրանցվել՝ մայիսի 12-ին: Այս դոմեյնն իր հերթին օգտատերերին վերաուղղորդում էր խաբեությամբ զբաղվող մի որևէ կայք, որը նման վարակների դեպքում սովորական մարտավարություն է:

Կայքում ավելացված օգտատիրոջը որոնելով՝ CyberHub-AM-ը պարզեց, որ կան բազմաթիվ այլ կայքեր, որոնք նույն կերպ են կոտրվել: Արագ ստուգումը հաստատեց, որ այս կայքերը նույնպես ուղղորդում էին դեպի scriptsplatform[.]com դոմեյն: Հաշվի առնելով, որ տուժած մյուս կայքերը որևէ առնչություն չունեին կազմակերպության հետ ո՛չ բովանդակությամբ, ո՛չ աշխարհագրորեն, CyberHub-AM-ը եզրակացրեց, որ սա պատահական հարձակում էր:

Ստուգելով WordPress-ի հաշվում ՀԿ-ի տեղադրած խրվակները՝ CyberHub-AM-ի մասնագետները գտան «Essential Addons for Elementor»-ը, որը կայքերի ստեղծման հանրահայտ Elementor խրվակի ընդարձակումն (անգլ.՝ extension) է: Այդ խրվակում վերջերս խոցելիություն էր հայտնաբերվել, ինչից կարելի է ենթադրել, որ դա էր կայքը կոտրելու հավանական պատճառը:[33]

Կարճ ժամանակ անց անվտանգությամբ զբաղվող Sucuri ընկերությունը վերլուծեց հենց այս խոցելիության միջոցով զանգվածային վարակների արշավը: Այդ զեկույցում տեղ գտած՝ օգտահաշիվները կոտրելու ցուցիչները հաստատում էին, որ հայկական կազմակերպությունն այս արշավի զոհն է դարձել:[34]

CyberHub-AM-ը հեռացրել է կեղծ «posts-layout» խրվակով թղթապանակը՝ վնասակար init.php, job.php ֆայլերով, ինչպես նաև որոշ քողարկված վեբշելներ (անգլ.՝ webshells): Թեև CyberHub-AM-ը հեշտությամբ մաքրեց վարակը, վեբկայքի կրկնակի վարակման կանխարգելման ապահովումը նույնքան հեշտությամբ չտրվեց: Որոշ կախվածությունների պատճառով չհաջողվեց թարմացնել Elementor խրվակի առանցքային ընդարձակումները՝ այնպես շտկելու խոցելիությունը, որ կայքի հիմնական գործունակությունը չխախտվի:

Առանց գործունակությունը խախտելու թարմացումներ իրականացնելու անկարողությունը, ցավոք, տարածված երևույթ է՝ հատկապես պատվերով պատրաստված կայքերի համար: Սա ցույց է տալիս, որ նման կայք վարելը շարունակական գործընթաց է, որը պահանջում է երկարաժամկետ սպասարկում: Ինչպես նշվում է CyberHub-AM-ի՝ միջադեպի վերլուծական գրառման մեջ, այնուամենայնիվ, «հայկական ընկերությունների մեծամասնությունն իրենց կայքերին վերաբերվում է ինչպես սառնարանի, որը կարելի է գնել, դնել խոհանոցում ու տարիներով մոռանալ դրա մասին»:[35]

Բարեբախտաբար, կազմակերպությունը նախատեսում էր գործարկել իր կայքի նոր տարբերակը դեպքից մի քանի շաբաթ անց, որը կլուծեր կախվածության հետ կապված խնդիրները: Մինչ այդ CyberHub-AM-ը տեղադրեց վեբ հասանելիության հրապատ (անգլ.՝ web access firewall, WAF)՝ հետագա սպառնալիքների ռիսկը մեղմելու համար: Կայքն այլևս չի կոտրվել:

## Pegasus լրտեսական ծրագիրն օգտագործվել է կին լրագրողի հեռախոսը կոտրելու համար

2022 թվականի նոյեմբերի 10-ին Աստղիկ Բեդևյանը նամակ ստացավ Apple-ից, որով նրան զգուշացնում էին, որ «պետության կողմից հովանավորվող հարձակում գործողները, հնարավոր է, թիրախավորում են [իր] iPhone-ը»:[36] Նա նման ահազանգ ստացած մի քանի հայաստանցիներից մեկն էր:

Բեդևյանը «Ազատ Եվրոպա/Ազատություն» (RFE/RL) ռադիոկայանի հայաստանյան ծառայության լրագրող է: 2020 թվականին նա լուսաբանել է Լեռնային Ղարաբաղի հակամարտությունը, իսկ 2021-ին՝ Հայաստանում կայացած արտահերթ խորհրդարանական ընտրությունները, որոնք մեծապես կենտրոնացած էին այդ հարցի վրա:[37]

Թեև Apple-ի ծանուցման մեջ նշված չէր, որ լրագրողի iPhone-ը վարակվել է, նա լրջորեն էր վերաբերվել նախազգուշացմանը՝ հեռախոսը հանձնելով CyberHub-AM-ին ստուգման համար: CyberHUB-AM-ի խորհրդին հետևելով՝ «Ազատություն» ռադիոկայանի երևանյան ծառայության բոլոր անդամների հեռախոսները ստուգվել են Amnesty Tech-ի կողմից: Amnesty Tech-ը, մանրազնին փորձաքննության ենթարկելով հեռախոսները, հաստատել է Pegasus-ով վարակված լինելու փաստը, որը տեղի է ունեցել 2021 թվականին՝ մոտավորապես ընտրությունների ժամանակ: Կոտրվել է նաև Բեդևյանի՝ «Ազատություն» ռադիոկայանի գործընկեր Կառլեն Ասլանյանի հեռախոսը:

Հայաստանում Pegasus-ի մասին առաջին փաստը արձանագրվել է 2021 թվականին, երբ լրտեսական ծրագիրը հայտնաբերվել է ինչպես իշխանության, այնպես էլ ընդդիմության մի քանի հանրաճանաչ քաղաքական գործիչների սարքերում:

Հարձակում գործողները Pegasus-ի միջոցով վարակել էին Արցախի Հանրապետության նախկին օմբուդսմանի, կառավարության մի խոսնակի և մի գիտնականի հեռախոսները:[38] Հետագայում պարզվեց, որ վարակված են եղել նաև մի հեռուստալրագրողի ու մի հանրաճանաչ իրավապաշտպանի սարքերը: Մի քանի այլ զոհեր նախընտրել են անանուն մնալ:

Թեպետ Pegasus-ը մշակած իսրայելական NSO Group ընկերությունը, ծրագիրը վաճառում է միայն կառավարություններին, հնարավոր չէ 100%-ով վստահ լինել, թե ով է այս արշավի հետևում կանգնած դերակատարը: Հայաստանում ծրագրերով վարակվելու վերաբերյալ իր զեկույցում, սակայն, Amnesty International-ը վկայակոչում է մեծածավալ անուղղակի ապացույցներ, որոնք վարակման այդ դեպքերը կապում են Ադրբեջանի հետ:[39] Citizen Lab-ն ավելի վաղ հայտնել էր իր կարծիքն այն մասին, որ Ադրբեջանում գոյություն ունի Pegasus-ի երկու օպերատոր, որոնցից մեկը կենտրոնացած է այդ երկրի ներսի, իսկ մյուսը՝ Հայաստանի վրա:[40]

Pegasus-ով հեռախոսի վարակվելու դեպքը Բեդևյանի վրա զգալի ազդեցություն է թողել, ընդ որում՝ ոչ միայն նրա լրագրողական աշխատանքի. հեռախոսը պարունակում էր նաև անձնական տվյալներ, այդ թվում՝ իր երեխաների մասին: Բեդևյանն այժմ գիտի, որ այլ երկրի իշխանություններին ամենայն հավանականությամբ հասանելի են դարձել այդ

տեղեկությունները: «Ես զգում եմ, որ իմ անձնական կյանքի գաղտնիությունը կոպտորեն խախտվել է», - ասել է նա Access Now-ին:[41]

Pegasus-ի վերաբերյալ վերլուծությունները և փաստագրումները հաճախ անտեսում են Pegasus-ով վարակված սարք ունենալու ազդեցությունը անձնապես զոհերի վրա, ինչն էլ ավելի ուժգին է զգացվում կանանց և այլ խոցելի խմբերի դեպքում: Ադրբեջանում մի կնոջ անձնական տվյալների արտահոսքը լուրջ նախազգուշացում է լրտեսական այն ծրագրերի հնարավոր հետևանքների մասին, որոնք մասնագիտական տվյալներից զատ հավաքում են անձնական տեղեկություններ: 2020 թվականին իշխանությունների մի հանրահայտ քննադատի կնոջ անձնական տվյալները՝ ներառյալ անունը, լուսանկարները և հեռախոսահամարը, հրապարակվել էին սոցիալական ցանցերում և էսկորտ ծառայությունների մի կայքում: Դրանից հետո իշխանամետ մամուլն օգտագործեց այդ տեղեկությունը՝ նրա դեմ արշավ սկսելու համար: Թեև գործը բացահայտ կերպով չի կապվել Pegasus-ի հետ, փաստերը վկայում են, որ տեղեկությունները հափշտակվել են նրա հեռախոսից:[42]

## Լրացուցիչ ընթերցանության նյութեր

Ինչպես ցույց է տալիս այս զեկույցը, քաղաքացիական հասարակության կազմակերպությունները և լրագրողները հաճախ բախվում են առանձնահատուկ, նորագույն սպառնալիքների՝ չունենալով դրանք հայտնաբերելու, վերլուծելու և կանխելու ռեսուրսներ: Քաղհասարակության և ԶԼՄ-ների առջև ծառացած սպառնալիքների խորը ընկալումը թույլ է տալիս թվային անվտանգության մասնագետներին հարմարեցնել իրենց արձագանքը և ավելի արդյունավետ աջակցել գործընկեր կազմակերպություններին՝ ստեղծելով մեղմման անհատականացված միջոցառումներ, որոնք ավելի ազդեցիկ են և ավելի հեշտ իրականացվող քաղհասարակության և լրատվամիջոցների համար: Քաղհասարակությանը և լրագրողներին սպառնալիքների մասին լրացուցիչ տեղեկություններ տրամադրելու համար Ինտերնյուսն իր գործընկերների հետ միասին հեղինակել է «Թվային սպառնալիքների համաշխարհային միտումները. քաղաքացիական հասարակություն և լրատվամիջոցներ» զեկույցը, ինչպես նաև Բրազիլիայում, Մեքսիկայում, Սերբիայում և Ուկրաինայում թվային սպառնալիքների լանդշաֆտի զեկույցները: Այս ռեսուրսները կարելի է գտնել Ինտերնյուսի կայքի «Տեխնոլոգիական ռեսուրսներ» էջում:

## Հայաստանի պատմությունը

Հայաստանի Հանրապետությունը ունիտար խորհրդարանական հանրապետություն է, որը գտնվում է Կովկասյան տարածաշրջանի Հայկական լեռնաշխարհում: Երկիրը սահմանակից է Թուրքիային, Վրաստանին, Ադրբեջանին, Իրանին և Ադրբեջանի Նախիջևան Էքսկլավին: Հայաստանը բազմադարյա պատմություն ունի, որը սկիզբ է առնում հնագույն ժամանակներից: Այն առաջին երկիրն է, որը 301 թվականին քրիստոնեությունը դարձրեց պետական կրոն:[43] Հայ

առաքելական եկեղեցին այսօր Հայաստանի ազգային եկեղեցին է: Հայերենը հնդեվրոպական լեզու է, որն ունի իր այբուբենը և չունի սերտ հարազատ լեզուներ:

Իր պատմության ընթացքի մեծ մասում այն տարածքը, որտեղ ապրել են հայերը, օտար պետությունների, մասնավորապես՝ պարսկական, օսմանյան և ռուսական կայսրությունների մաս է կազմել: Առաջին համաշխարհային պատերազմի ժամանակ ռուսական բանակում հայ կամավորականների ծառայության վերաբերյալ օսմանյան կառավարության կասկածը հանգեցրեց 1-ից 1,5 միլիոն հայերի զանգվածային սպանությունների: Թեև գիտնականների մեծամասնությունը դա համարում է ցեղասպանություն, այն շարունակում է շատ վիճելի թեմա մնալ Թուրքիայում, որը չի ճանաչում ցեղասպանությունը. այդ հարցն այսօր էլ լարված է պահում Հայաստանի և Թուրքիայի հարաբերությունները:[44]

Կարճատև անկախ պետականությունից հետո երկիրը մաս կազմեց Խորհրդային Միության՝ իբրև Հայկական Խորհրդային Սոցիալիստական Հանրապետություն՝ մնալով այդպիսին մինչև 1991 թվականին անկախության հռչակումը:[45]

Freedom House-ը 2017 թվականին Հայաստանը դասակարգել է իբրև «փափուկ ավտորիտար միտումներ» ունեցող երկիր՝ տալով նրան 100-ից 45 միավոր և շնորհելով «մասամբ ազատ» վարկանիշ:[46] 2018-ի բողոքի զանգվածային ցույցերի ճնշման տակ կառավարությունը հրաժարական տվեց: Նրան փոխարինեց նոր վարչակազմ, որը խոստանում էր պայքարել կոռուպցիայի դեմ և հաստատել ավելի ժողովրդավարական համակարգ: 2023 թվականի զեկույցի տվյալներով՝ Հայաստանն այժմ ունի 100-ից 54 միավոր: Նոր կառավարությունը իշխանությունը ստանձնելուց ի վեր բախվել է մի քանի ճգնաժամերի, այդ թվում՝ COVID-19-ի համավարակի բռնկումը, 2020 թվականին Լեռնային Ղարաբաղի երկրորդ պատերազմը, իսկ տակավին վերջերս՝ Ադրբեջանի կողմից Լեռնային Ղարաբաղի գրավումը:[47]

Հայաստանը Համաշխարհային բանկի կողմից[48] դասակարգվում է որպես միջինից բարձր եկամուտ ունեցող տնտեսություն և աշխարհաքաղաքական առումով ավելի ու ավելի է մերձենում Եվրոպային՝ չնայած իր աշխարհագրական դիրքին: Հայաստանը ՄԱԿ-ի,[49] Եվրոպայի խորհրդի[50] և Առևտրի համաշխարհային կազմակերպության[51] անդամ է: Այն անդամակցում է նաև մի քանի եվրասիական կազմակերպությունների, ինչպիսիք են Անկախ պետությունների համագործակցությունը[52], Ասիական զարգացման բանկը[53] և Հավաքական անվտանգության պայմանագրի կազմակերպությունը:[54]

## Երախտիքի խոսք

2021 թվականից Ինտերնյուսն աշխատել է սպառնալիքներով զբաղվող յոթ լաբորատորիաների հետ *(անգլ.՝ Threat Labs. տեղական կազմակերպություններ, որոնք ունեն կասկածելի ֆիշինգի և վնասակար ծրագրերի նմուշները վերլուծելու և այնուհետև հարձակումների միտումների, ծագող սպառնալիքների և հակազդեցությունների վերաբերյալ համայնքին տեղեկություններ տրամադրելու տեխնիկական կարողություններ և համապատասխան գործիքներ)՝* արձագանքելու այն միջադեպերին, որոնք ազդում են ողջ աշխարհով մեկ քաղաքացիական

հասարակության և մեդիա կազմակերպությունների թվային անվտանգության վրա: Միջադեպերին արձագանքելու ծրագրի միջոցով հավաքված տվյալները օգնել են մշակելու ռիսկային գոտում գտնվող համայնքների համար մեղմման հնարքներ և արձագանքման մոտեցումներ, իչպես նաև տեղեկություններ են տրամադրել այս զեկույցը կազմելու համար:

Ինտերնյուսն իր երախտագիտությունն է հայտնում սպառնալիքներով զբաղվող լաբորատորիաների համայնքին, որը մեզ հետ աշխատել է այս նախագծի վրա: Նրանք հանձնառու են օգնելու կարիք ունեցողներին և երաշխավորելու, որ քաղաքացիական հասարակության և լրատվամիջոցների իրենց գործընկերները կարողանան անվտանգ և արդյունավետ կերպով ավարտին հասցնել իրենց կարևոր աշխատանքը: Ընդհանուր առմամբ, այս ծրագրի աջակցությամբ սպառնալիքներով զբաղվող լաբորատորիաները արձագանքել են թվային անվտանգության ավելի քան 200 միջադեպերի և հրապարակել ավելի քան 60 կրթական ռեսուրսներ իրենց կայքերում և սոցիալական մեդիա հարթակներում:

Հատուկ շնորհակալություն ենք հայտնում CyberHub-AM-ին այս պրակտիկ օրինակների փաստագրման և տարածման համար տեղեկություններ տրամադրելու, ինչպես նաև այս զեկույցի նախագիծն ընթերցելու և արժեքավոր նկատառումներ հայտնելու համար: Զեկույցն իրականություն չէր դառնա առանց Յանա Ղահրամանյանի, Սամվել Մարտիրոսյանի և Արթուր Պապյանի:

# Ծանոթագրություններ

[1] "Explainer: What is Nagorno-Karabakh and why are tensions rising?" *Al Jazeera.* April 24, 2023. https://www.aljazeera.com/news/2023/4/24/explainer-what-is-nagorno-karabakh-why-are-tensions-rising

[2] Ertl, Michael. "Nagorno-Karabakh: Conflict between Azerbaijan and Armenians explained." BBC News. September 28, 2023

[3] Bazail-Emil, Eric and Gabriel Gavin. "Blinken warned lawmakers Azerbaijan may invade Armenia in coming weeks." Politico. October 13, 2023. https://www.politico.com/news/2023/10/13/blinken-warned-lawmakers-azerbaijan-may-invade-armenia-in-coming-weeks-00121500

[4] Amiryan, Tigran and Anna Sokolova. "Relocated Russian Democracy - A View from Armenia." Heinrich Böll Stiftung. June 1, 2022. https://ge.boell.org/en/2022/06/01/relocated-russian-democracy-view-armenia

[5] Tatikyan, Sossi. "The Context Behind Armenia's UN Vote on Ukraine." *EVN Report*. March 3, 2022. https://evnreport.com/politics/the-context-behind-armenias-un-vote-on-ukraine/

[6] Atasuntsev, Alexander. "Long-Standing Ties Between Armenia and Russia Are Fraying Fast." Carnegie Endowment for International Peace. October 13, 2023. https://carnegieendowment.org/politika/90768

[7] "Freedom in the World 2023: Armenia." Freedom House. վերջին մուտքը՝ 2023թ. հուլիս https://freedomhouse.org/country/armenia/freedom-world/2023

[8] Նույն տեղում

[9] "Armenia." Reporters Without Borders. վերջին մուտքը՝ 2023թ. հուլիս. https://rsf.org/en/country/armenia.

[10] "Armenia must drop 'intimidating' criminal charges against minority rights activist – UN experts." United Nations, OHCHR Press Release. August 10, 2021. https://www.ohchr.org/en/press-releases/2021/08/armenia-must-drop-intimidating-criminal-charges-against-minority-rights

[11] Chilingaryan, Anahit. "High Stakes for Armenian Democracy in Rights Defender's Trial." Human Rights Watch. June 21, 2022. https://www.hrw.org/news/2022/06/21/high-stakes-armenian-democracy-rights-defenders-trial

[12] "Public opinion toward LGBT people in Yerevan, Gyumri and Vanadzor cities." We and Our Rights. 2011. https://issuu.com/pinkarmenia/docs/lgbtsurveyen/9?e=3748946/2746746

[13] "LGBT activist Mamikon Hovespyan announced as equality award winner for 2017." Equal Rights Trust. July 25, 2017. https://www.equalrightstrust.org/news/lgbt-activist-mamikon-hovespyan-announced-equality-award-winner-2017; Pilishvili, Catherine. "Another Change to Address Homophobic Violence in Armenia." Human Rights Watch. August 28, 2020. https://www.hrw.org/news/2020/08/28/another-chance-address-homophobic-violence-armenia

[14] "LGBT activist Mamikon Hovespyan announced as equality award winner for 2017," Equal Rights Trust.

[15] Papyan, Artur. "Internet penetration rate has declined in Armenia in 2020 according to ITU." *The Armenian Observer Blog*. October 16, 2020. https://ditord.com/2020/10/internet-penetration-rate-has-declined-in-armenia-in-2020/

[16] Ranum, Marcus J. "FUDwatch: Armenia." Tenable. May 3, 2013. https://www.tenable.com/blog/fudwatch-armenia

[17] "Russian spam mastermind jailed for creating botnet." *BBC*. May 24, 2012. https://www.bbc.com/news/technology-18189987

[18] “Armenia police warn of growing cybercrime rate.” *Armenpress*. վերջին փոփոխությունը՝ 2018թ. հունիսի 12. https://armenpress.am/eng/news/937066/

[19] “Armenian police bust Yerevan-based cybercrime syndicate targeting U.S. users via tech support scam.” *Armenpress.* վերջին փոփոխությունը՝ 2019թ. մայիսի 1. https://armenpress.am/eng/news/973297.html

[20] Faou, Matthieu. “Tracking Turla: New backdoor delivered via Armenian watering holes.” We Live Security, ESET Research. March 12, 2020. https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/

[21] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert. “Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus.” The Citizen Lab. July 15, 2021. https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

[22] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert. “Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus.” The Citizen Lab. July 15, 2021. https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

[23] Stone, Maddie and Clement Lecigne. “How we protect users from 0-day attacks.” Google, Threat Analysis Group. July 14, 2021. https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/

[24] Տեղեկությունը՝ CyberHub-AM-ի

[25] Միջադեպի արձագանքի վերաբերյալ տեղեկությունը՝ CyberHub-AM-ի

[26] Միջադեպի արձագանքի վերաբերյալ տեղեկությունը՝ CyberHub-AM-ի

[27] Dvilyanski, Mike, David Agranovich, and Nathaniel Gleicher. “Threat Report on the Surveillance-for-Hire Industry.” Meta. December 16, 2021. https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

[28] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert. “Pegasus vs. Predator: Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware.” The Citizen Lab. December 16, 2021. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[29] “Review of Attacks Against Armenian Telegram Users in Recent Months.” CyberHUB. վերջին փոփոխությունը՝ 2022թ. օգոստոսի 26. https://cyberhub.am/en/blog/2022/08/26/review-of-attacks-against-armenian-telegram-users-in-recent-months/

[30] “Arsen Babayan: How authorities infect victims’ phones with Pegasus spyware.” *Panorama*. Վերջին փոփոխությունը՝ 2021թ. նոյեմբերի 27. https://www.panorama.am/en/news/2021/11/27/Arsen-Babayan/2604970

[31] Krapiva, Natalia, and Giulio. “Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict.” Access Now. May 25, 2023. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/

[32] RFE/RL. “Azerbaijan Suspected Of Spying On Reporters, Activists By Using Software To Access Phones.” RadioFreeEurope RadioLiberty. վերջին փոփոխությունը՝ 2021թ. հուլիսի 18. https://www.rferl.org/a/azerbaijan-pegasus-spying-nso/31365076.html

[33] Muhammad, Rafie. “Critical Privilege Escalation in Essential Addons for Elementor Plugin Affecting 1+ Million Sites.” Patchstack. վերջին փոփոխությունը՝ 2023թ. մայիսի 11. https://patchstack.com/articles/critical-privilege-escalation-in-essential-addons-for-elementor-plugin-affecting-1-million-sites/

[34] Martin, Ben. “Vulnerability in Essential Addons for Elementor Leads to Mass Infection.” *SucriBlog*. վերջին փոփոխությունը՝ 2023թ. մայիսի 18. https://blog.sucuri.net/2023/05/vulnerability-in-essential-addons-for-elementor-leads-to-mass-infection.html

[35] “Hackers leverage vulnerability of Essential Addons plugin to exploit Armenian WordPress sites.” CyberHUB. վերջին փոփոխությունը 2023թ. մայիսի 23. https://cyberhub.am/en/blog/2023/05/23/hackers-leverage-vulnerability-of-the-essential-addons-plugin-to-exploit-armenian-wordpress-sites/

[36] "Armenia: Azerbaijan Hacks Armenian Journalist Astghik Bedevyan’s Phone During War.” Coalition For Women in Journalism. May 29, 2023. https://www.womeninjournalism.org/threats-all/armenia-azerbaijan-hacks-armenian-journalist-astghik-bedevyans-phone-during-war

[37] “Armenia PM Pashinyan’s Civil Contract claims victory in snap poll.” *Al Jazeera.* June 21, 2021. https://www.aljazeera.com/news/2021/6/21/armenia-nikol-pashinyan-claims-victory-in-snap-polls

[38] Krapiva, Natalia, and Giulio. “Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict.” Access Now. May 25, 2023. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/

[39] “Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict.” Amnesty International. May 25, 2023. https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/

[40] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Nicola Lawford, and Ron Deibert. “Armenia-Azerbaijan conflict: Pegasus infections – Technical Brief [1].” The Citizen Lab. May 25, 2023. https://citizenlab.ca/2023/05/cr1-armenia-pegasus/

[41] Krapiva, “Hacking in a war zone: Pegasus spyware in Azerbaijan-Armenia conflict.”

[42] Patrucic, Miranda and Kelly Bloss. “Life in Azerbaijan’s Digital Autocracy: ‘They Want to be in Control of Everything.’” Organized Crime and Corruption Reporting Project. July 18, 2021. https://www.occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything

[43] “Armenia country profile.” *BBC*. վերջին փոփոխությունը՝ 2023թ. հուլիսի 3. https://www.bbc.com/news/world-europe-17398605

[44] Նույն տեղում

[45] Նույն տեղում

[46] “Freedom in the World 2017: Armenia.” Freedom House. վերջին մուտքը՝ 2023թ. հուլիս. https://freedomhouse.org/country/armenia/freedom-world/2017

[47] “Armenia country profile,” *BBC*

[48] “Middle income.” The World Bank, Data. վերջին մուտքը՝ 2023թ. հուլիս. https://data.worldbank.org/country/XP

[49] “Member States.” United Nations. վերջին մուտքը՝ 2023թ. հուլիս. https://www.un.org/en/about-us/member-states

[50] “46 Member States.” Council of Europe. վերջին մուտքը՝ 2023թ. հուլիս. https://www.coe.int/en/web/portal/46-members-states

[51] “Members and Observers.” World Trade Organization. վերջին մուտքը՝ 2023թ. հուլիս. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm

[52] “Commonwealth of Independent States.” *Britannica*. վերջին մուտքը՝ 2023թ. հուլիս. https://www.britannica.com/topic/Commonwealth-of-Independent-States

[53] “Who We Are.” Asian Development Bank. վերջին մուտքը՝ 2023թ. հուլիս. https://www.adb.org/who-we-are/about

[54] “Countries.” Collective Security Treaty Organization. վերջին մուտքը՝ 2023թ. հուլիս. https://en.odkb-csto.org/countries/