



HAL
open science

Arestakes Simavoryan

► **To cite this version:**

Arestakes Simavoryan.
03689136

. 2019, 10.5281/zenodo.6559021 . hal-

HAL Id: hal-03689136

<https://hal.science/hal-03689136>

Submitted on 27 Jul 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright



Turkey's cyber security policy

Arestakes Simavoryan

Specialist of Oriental Studies, Turkologist, ORBELI - Analytical Research Center, Analytical Senior expert of the service

ARTICLE INFO

Article history:

Received 06.10. 2019

Available online
 06.16, 2019

Keywords:

Turkey,
 cyber security
 cyber education
 Internet:

ABSTRACT

Cybersecurity is a problem for every country today, as the spread of the Internet has deepened and fragmented security issues. It is no coincidence that the penetration of the Internet into various spheres of public life forces state and public actors to pay close attention to defense measures, and cybersecurity has become an integral part of the national security of states. Many countries have adopted different concepts and strategies for regulating the sector. In this regard, Turkey is actively working, where cyber threats have posed new security challenges for the country.

DOI:<https://doi.org/10.5281/zenodo.6559021>

© 2022 All Rights Reserved

Թուրքիայի կիբեռանվտանգության քաղաքականությունը

Արեստակես Միմավորյան

Հիմնաբառեր:

Թուրքիա,
 կիբեռանվտանգություն,
 կիբեռկրթություն,
 համացանց

ՀԱՄԱՌՈՏԱԳԻՐ

Կիբեռանվտանգությունն այսօր մարտահրավեր է յուրաքանչյուր պետության համար, քանի որ համացանցի ընդլայնումը հանգեցրել է անվտանգային խնդիրների խորացմանն ու շերտավորմանը: Պատահական չէ, որ համացանցային կապի ներթափանցումը հանրային կյանքի տարբեր բնագավառներ պետական և հանրային սուբյեկտներին հարկադրում է մեծ ուշադրություն դարձնել պաշտպանական միջոցառումներին, իսկ կիբեռանվտանգությունը դարձել է պետությունների ազգային անվտանգության անքակտելի մասը: Ոլորտի կանոնակարգման նպատակով բազմաթիվ երկրներ ընդունել են տարաբնույթ հայեցակարգեր և ռազմավարություններ: Այս առումով բավական ակտիվ աշխատանքներ է անում նաև Թուրքիան, որտեղ կիբեռապառնալիքներն անվտանգային նոր մարտահրավերների առաջ են կանգնեցրել երկիրը:

Կիրառական տնտեսագիտության և մարտահրավեր է յուրաքանչյուր պետության համար, քանի որ համացանցի ընդլայնումը հանգեցրել է անվտանգային խնդիրների խորացմանն ու շերտավորմանը: Պատահական չէ, որ համացանցային կապի ներթափանցումը հանրային կյանքի տարբեր բնագավառներ պետական և հանրային սուբյեկտներին հարկադրում է մեծ ուշադրություն դարձնել պաշտպանական միջոցառումներին, իսկ կիրառական տնտեսագիտությունը դարձել է պետությունների ազգային անվտանգության անքակտելի մասը: Ոլորտի կանոնակարգման նպատակով բազմաթիվ երկրներ ընդունել են տարաբնույթ հայեցակարգեր և ռազմավարություններ: Այս առումով բավական ակտիվ աշխատանքներ է անում նաև Թուրքիան, որտեղ կիրառական տնտեսագիտության անվտանգային նոր մարտահրավերների առաջ են կանգնեցրել երկիրը:

Կիրառական տնտեսագիտության և մարտահրավերի անվտանգության քաղաքականություն մշակողների ուշադրության կենտրոնում են դեռևս 1990-ականներին վերջից: Պետական միասնական քաղաքականության մշակումը հրամայական դարձավ, և Թուրքիայի պետական տնտեսագիտության մարմինները սկսեցին զբաղվել ինչպես տեղեկատվական համակարգերի ու կիրառական տնտեսագիտության ենթակառուցվածքների պաշտպանությամբ, այնպես էլ դրանց հետ անմիջականորեն փոխկապակցված, խոցելի համարվող ենթակառուցվածքների պաշտպանության բարձրագույն ու կատարելագործմամբ: Կիրառական տնտեսագիտությունը կարևորվեց նաև տեղեկատվական համակարգերի վրա լոկալ ու անդրսահմանային կիրառական տնտեսագիտության, կիրառական տնտեսագիտության իրավունքների պաշտպանության և տարատեսակ կիրառական տնտեսագիտությունների աճի պայմաններում [Симаворян, 2018; Հարությունյան և ուրիշ., 2018; 341]:

2013թ. ընդունվեց կիրառական տնտեսագիտության վերաբերյալ առաջին ռազմավարական փաստաթուղթը՝ «Ազգային կիրառական տնտեսագիտության ռազմավարությունը և 2013-2014թթ. գործողությունների պլան»-ը, որը առավելապես վերաբերում էր ոլորտի անվտանգությունն ապահովող կառույցների ստեղծմանը¹:

Արդյունքում 2013թ. ստեղծվում է **Կիրառական տնտեսագիտության խորհուրդ** և Կիրառական տնտեսագիտության հարցերի ղեկավարի ազգային կենտրոն՝ պետական և մասնավոր հաստատությունների անվտանգությունն ապահովող իր կիրառական տնտեսագիտության Երկրորդ հստակեցվում էին պետության համար առաջնահերթ նշանակություն ունեցող այն ոլորտները (էներգետիկա, ջրային կառավարում և այլն), որոնց ենթակառուցվածքները (էլեկտրացանցեր, ջրամատակարարման համակարգեր) համարվում էին կրիտիկական և ունեին պետական կիրառական տնտեսագիտության կարիք:

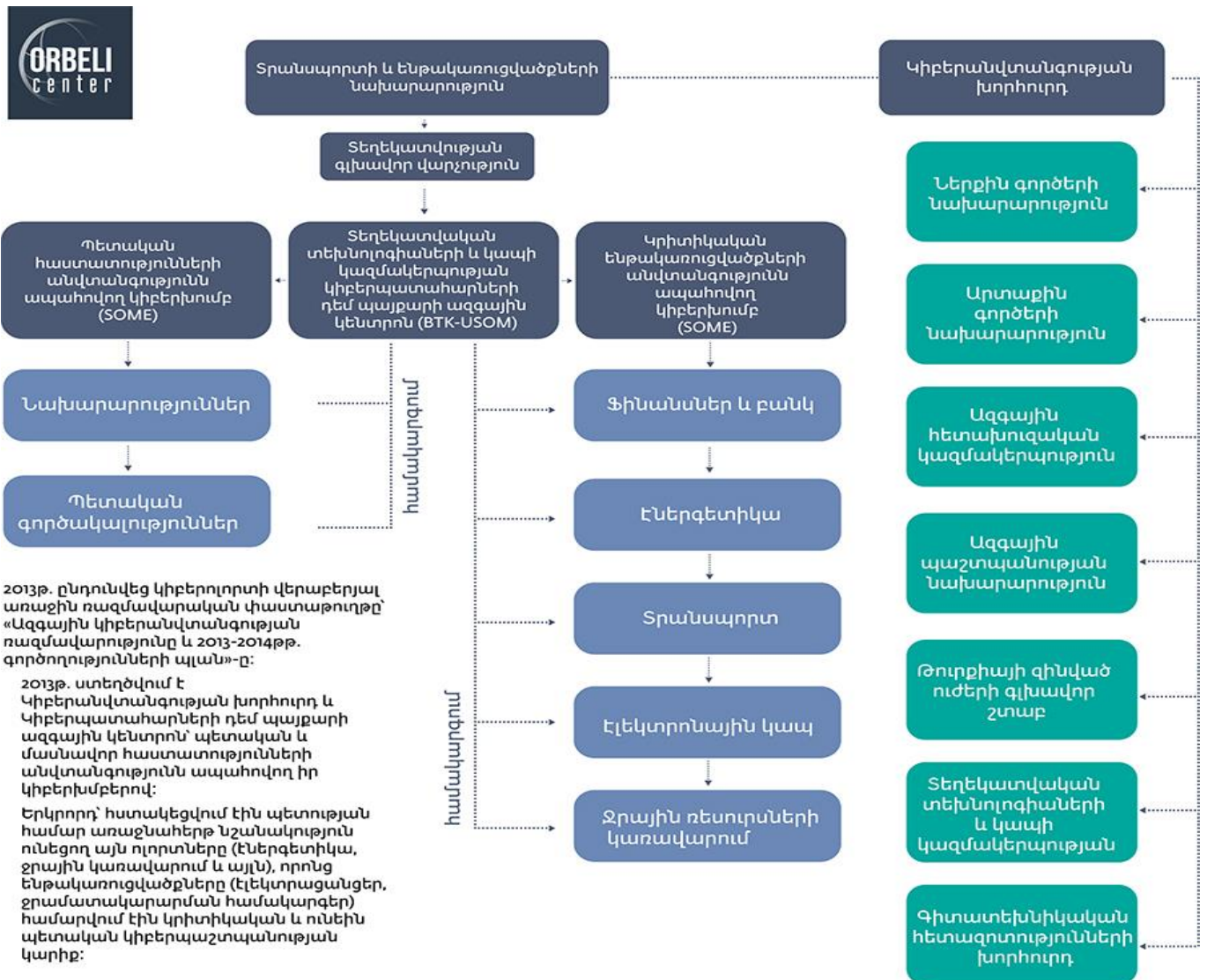
Մյուս կարևորագույն հարցերը էական նշանակություն ունեին ոլորտի հետագա զարգացումն ապահովելու տեսանկյունից: Հատկապես հրատապ էր համարվում անվտանգության մասնագետների պատրաստումը, ուսումնակրթական բազայի ստեղծումն ու ազգային կիրառական տնտեսագիտության զարգացումը, միջազգային փոխգործակցությունը և այլն: Հարկ է նաև նշել, որ Թուրքիայի կառավարության 2012թ. հոկտեմբերին ընդունած որոշումով² կիրառական տնտեսագիտության բոլոր բաղադրիչների ապահովումը, որը մինչ այդ իրականացնում էր

¹ Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013, <https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-planı-2013-2014-5a3412cf8f45a.pdf>

² <https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf>



Թուրքիայի գիտատեխնիկական հետազոտությունների խորհուրդը (TÜBİTAK), դրվում է տրանսպորտի և ենթակառուցվածքների նախարարության վրա, որը կարող է ձևավորել աշխատանքային խմբեր՝ պարտականությունների իրականացման համար: Գերատեսչական կառույցներն ու պետական գործակալությունները պարտավոր են հետամուտ լինել Կիբերանվտանգության խորհրդի մշակած քաղաքականությանն ու չափանիշներին, որոնք բխում են Ազգային կիբերանվտանգության ռազմավարությունից: Խորհուրդի կազմում ընդգրկված են ուժային կառույցների ղեկավարները կամ տեղակալները: Կիբերպաշտպանության ոլորտում կարևոր դերակատարություն ունի «Տեղեկատվական տեխնոլոգիաների և կապի կազմակերպության» կիբերպատահարների դեմ պայքարի ազգային կենտրոնը (BTK-USOM), որի շրջանակներում գործում են պետական հաստատությունների և կրիտիկական համարվող ենթակառուցվածքների անվտանգությունն ապահովող կիբերխմբերը (Գրաֆիկ1):





2016թ. տրանսպորտի և ենթակառուցվածքների նախարարությունը հրապարակեց «Ազգային կիբերանվտանգության ռազմավարություն և 2016-2019թթ. գործողությունների պլան» նոր փաստաթուղթը³ : Հաշվի առնելով ոլորտի ռիսկերը և հետևելով ռազմավարությունում ամրագրված նպատակներին, պատասխանատու մարմինները պետք է՝

- հաշվարկեն կիբերհարձակումների ազդեցությունը, ձեռնարկեն անհրաժեշտ պաշտպանական գործողություններ, ինչպես նաև օժանդակեն իրավապահ ու պետական այլ մարմիններին՝ կիբերհանցագործությունների հետաքննության և դատավարության համար,
- ձեռնարկեն քայլեր տեղեկատվական համակարգերի և նոր ենթակառուցվածքների ստեղծման ուղղությամբ,
- ապահովեն տեղեկատվական տեխնոլոգիաների տիրույթում առկա բոլոր սվյալների, ծառայությունների, գործարքների, համակարգերի անվտանգությունն ու գաղտնիությունը:

Բացի դրանից, նախարարություններն ու պետական գործակալությունները պարտավոր են գնահատել իրենց ոլորտներում առկա և հնարավոր զարգացումներով պայմանավորված ռիսկերը, քարտեզագրել և հաշվառել Թուրքիայի տարածքում գտնվող, կրիտիկական ոլորտներում ներառված օբյեկտները՝ տալով դրանց քանակական և որակական բնութագրիչները: Այլ կարևոր հարցերից են նաև կիբերհանցագործությունների դեմ պայքարի ուժեղացումն ու տեղեկատվական-հաղորդակցական տեխնոլոգիաների նորացումը:

ԿԻԲԵՐԿՐԹՈՒԹՅԱՆ ՀԱՐՑԵՐԸ

Համաձայն միջազգային գնահատականների՝ ռազմավարական մակարդակով իրագործվող քաղաքականության շնորհիվ Թուրքիան կիբերանվտանգության ոլորտում տարեցտարի բարելավում է իր դիրքերը: 2018թ. կիբերանվտանգության գլոբալ ինդեքսում (Global Cybersecurity Index – GCI) Թուրքիան 20-րդ տեղում է⁴:

Վարկանիշային զեկույցի մեթոդաբանությունը հիմնվում է մոտ 25 չափորոշիչների վրա, որոնք իրենց հերթին դասակարգված են հինգ խմբերով: Դրանք են՝ ոլորտը կարգավորող օրենսդրական դաշտը, տեխնիկական բազան, կազմակերպչական հարցերը, կրթական և միջազգային համագործակցության շրջանակները: Ինչպես տեսնում ենք, փորձագետները որևէ պետության կիբերքաղաքականությունը գնահատելիս չափորոշիչների շարքում որպես կարևոր ցուցիչ նկատի են առնում նաև կրթական բաղադրիչը: Այս տեսանկյունից Թուրքիայի կիբերանվտանգության վերաբերյալ փաստաթղթերում ընդգծվում է անհրաժեշտ թվով և անվտանգության մշակույթին (safety culture) տիրապետող, որակյալ մասնագիտական ուժերի կազմավորման հարցը: Թուրքական «Havelsan» ռազմարդյունաբերական ընկերության

³ 2016-2019 ulusal siber guvenlik stratejisi, <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf>
⁴ Համեմատության համար նշենք, որ Ադրբեջանն ու Հայաստանը համատասխանաբար գտնվում են՝ 55 և 79-րդ տեղերում:

նախկին փոխսոսերեն Յ. Բադրըաչըքի խոսքերով⁵, Թուրքիան կիրքերանվտանգության շուրջ 20.000 մասնագետների կարիք ունի: Այդ պատճառով կիրքերկրթության կազմակերպման նկատմամբ ուշադրությունն ու հետաքրքրությունը չափազանց մեծ է, որին մասնակից են պետական և մասնավոր հատվածի զանազան դերակատարներ:

Համաձայն հետազոտողների՝ տեղեկատվական անվտանգության ոլորտում կրթական ծառայությունները գլխավորապես տրամադրվում են մասնավոր ընկերությունները ⁶ : Այդուհանդերձ, բարձր որակավորում ունեցող անձնակազմի պատրաստման և պետության պահանջներին համապատասխանող բավարար թվով մասնագետների ամենահամապատասխան հաստատությունները բուհերն են: «Կիրքերանվտանգություն» առարկան դասավանդվում է հիմնականում տեխնիկական գիտությունների բնագավառում կրթություն տրամադրող համալսարաններում [Sevri, Topaloglu, 2016; 928], նաև ռազմակրթական նշանակության որոշ ինստիտուտներում⁷:

Պետական հաստատությունների շարքում էական է Թուրքիայի գիտատեխնիկական հետազոտությունների խորհրդին կից գործող Կիրքերանվտանգության ինստիտուտի դերը: Համակարգչային տեխնոլոգիաների տեխնիկական անվտանգությունն ապահովելու, կիրքեսպառնալիքները նվազագույնի հասցնելու համար ինստիտուտը պատրաստում է ցանցային և տեղեկատվական անվտանգության կառավարման, տեղեկատվական համակարգերի վերահսկման և ստուգման, կրիտիկական ենթակառուցվածքների և այլ ենթաուղղությունների մասնագետներ ⁸, տեղեկատվական համակարգերով է ապահովում ռազմական և հանրային նշանակության կազմակերպություններին, տրամադրում խորհրդատվություն: Հարկ է ընդգծել, որ 2018թ. սեպտեմբերին ինստիտուտը ՆԱՏՕ-ի SPS (Գիտությունը հանուն խաղաղության և անվտանգության) ծրագրի շրջանակներում ⁹ Ադրբեջանի մասնագետների համար Բաքվում կազմակերպել է «Ընդլայնված կիրքերպաշտպանության վերապատրաստման դասընթաց»:

Այս քաղաքականությունից անմասն չի մնում նաև ռազմական ոլորտը, ինչի մասին վկայում է 2018թ. կիրքերանվտանգության ուսանողական մրցաշարին Թուրքիայի պաշտպանական արդյունաբերության գլխավոր վարչության քարտուղար Ի. Դեմիրի հայտարարությունը, որ Թուրքիան նպատակադրվել է առաջատար դիրքեր զբաղեցնել այս ոլորտում՝ ոչ միայն դիմակայելով կիրքերհարձակումներին, այլև անհրաժեշտության դեպքում համարժեք գործողություններ նախաձեռնելով ¹⁰ : Նշենք, որ մասնագետներ են վերապատրաստում նաև ռազմական կառույցները, օրինակ՝ «Havelsan» ռազմարդյունաբերական ընկերությանը, որը դասընթացներ է կազմակերպում տարբեր առարկաներով և ուղղություններով, ներառյալ ավիացիոն ու ռադիոէլեկտրոնային պայքարը՝ օգտագործելով ընկերությանն ենթակա «Կիրքերանվտանգության գործողությունների կենտրոնի» և «Կիրքերանվտանգության ակադեմիայի» իր աշխատակիցների փորձառությունը:

⁵ 20 bin siber güvenlik elemanına ihtiyaç var, <https://www.trthaber.com/haber/turkiye/20-bin-siber-guvenlik-elemanina-ihitiyac-var-241392.html>

⁶ <https://www.bilgeadam.com/akademi>, <https://www.bilgiguvenligi.org.tr/>, <https://sibertime.com.tr/>

⁷ <http://www.hezarfen.hho.edu.tr/>

⁸ տե՛ս, Կիրքերանվտանգության կրթական պորտալ, <https://egitim.sge.gov.tr/>

⁹ <https://sge.bilgem.tubitak.gov>

¹⁰ Турция рассчитывает стать лидером в сфере кибербезопасности, <https://rusturkey.com>



Թուրքիայի պետական քաղաքականության ձևավորմանը մասնակցում են բազմաթիվ կազմակերպություններ, որոնցից են՝

- Անձնական տվյալների պաշտպանության պետական կազմակերպությունը,
- Պաշտպանական արդյունաբերության Կիբերպաշտպանության գործողությունների կենտրոնն ու Կիբերանվտանգության խումբը,
- Ներքին գործերի նախարարության կիբերհանցագործությունների դեմ պայքարի վարչությունը,
- Թուրքիայի նախագահին առընթեր «Թվային փոխակերպման» գրասենյակը,
- Ազգային հետախուզական կազմակերպության Էլեկտրոնային և տեխնիկական հետախուզության վարչությունը,
- Թուրքիայի զինված ուժերի կիբերպաշտպանության հրամանատարությունը¹¹ն այլն:

Ամփոփելով նշենք, որ տեղեկատվական անվտանգության 2016-2019թթ. ռազմավարությունը ամբողջությամբ չի ներկայացնում կիբերանվտանգության հետ առնչվող մարտահրավերներն ու ռիսկերը, նաև պետական և հանրային սեկտորի այն դերակատարներին, որոնք աջակցում են պետական քաղաքականությանը: Մինևույն ժամանակ, ինչպես նշված է փաստաթղթում, ռազմավարության և գործողությունների պլանը պետք է թարմացվի՝ տեխնոլոգիաների արագընթաց զարգացմանն ու ոլորտի կարգավորումներին զուգընթաց, և նոր ռազմավարության մշակումը չի բացառվում:

References

1. Sevri, M., Topaloğlu, N. (2016). Türkiye’de siber güvenlik eğitiminin durumu. *International Conference on Education in Mathematics, Science & Technology (ICEMST)*, s.928 .
2. Симаворян, А. (2018). Подходы к критическим инфраструктурам в Турции. *Глобус*, 7 (96), 4-9.
3. Հարությունյան, Գ., Մարջանյան, Ա., Վերանյան, Կ., Մինավորյան, Ա., Հովյան, Վ., Մանուկյան, Ս., Թևիկյան, Ա. (2018). *Critical Infrastructures and National Security [Կրիտիկական Ենթակառուցվածքներ Եւ Ազգային Անվտանգություն]* (No. hal-03548161).

¹¹ Գործում է Թուրքիայի զինված ուժերի գլխավոր շտաբի Կապի, էլեկտրոնիկայի և տեղեկատվական համակարգերի տնօրինության (MEBS) ներքո: