ORBELI –
Центр аналитических исследований
ORBELI - Analytical Research Center–
Home page: https://orbeli.am/

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.

© 2022 All Rights Reserved

Թուրքիայի կիբերանվտանգության քաղաքականությունը

Արեստակես Սիմավորյան

Հիմնաբառեր:
Թուրքիա,
կիբերանվտանգություն,
կիբերկրթություն,
համացանց

ՀԱՄԱՌՈՏԱԳԻՐ

Կիբերանվտանգությունն 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 կիբերանվտանգությունը 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 կիբերսպառնալիքներն անվտանգային նոր մարտահրավերների առաջ են կանգնեցրել երկիրը:

Կիբերանվտանգությունն 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 կիբերանվտանգությունը 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 կիբերսպառնալիքներն անվտանգային նոր մարտահրավերների առաջ են կանգնեցրել երկիրը:

Կիբերոլորտի ռիսկերը Թուրքիայի անվտանգության քաղաքականություն մշակողների ուշադրության կենտրոնում են դեռևս 1990-ականներին վերջից: Պետական միասնական քաղաքականության մշակումը հրամայական դարձավ, և Թուրքիայի պետանվտանգության մարմինները սկսեցին զբաղվել ինչպես տեղեկատվական համակարգերի ու կիբերանվտանգության ենթակառուցվածքների պաշպանությամբ, այնպես էլ դրանց հետ անմիջականորեն փոխկապակցված, խոցելի համարվող ենթակառուցվածքների պաշտպանունակության բարձացմամբ ու կատարելագործմամբ: Կիբերանվտանգությունը կարևորվեց նաև տեղեկատվական համակարգերի վրա լոկալ ու անդրսահմանային կիբերհարձակումների, կիբերտիրույթում հեղինակային իրավունքների պաշտպանության և տարատեսակ կիբերհանցագործությունների աճի պայմաններում **[Симаворян, 2018; Հարությունյան և ուրիշ., 2018; 341]:**

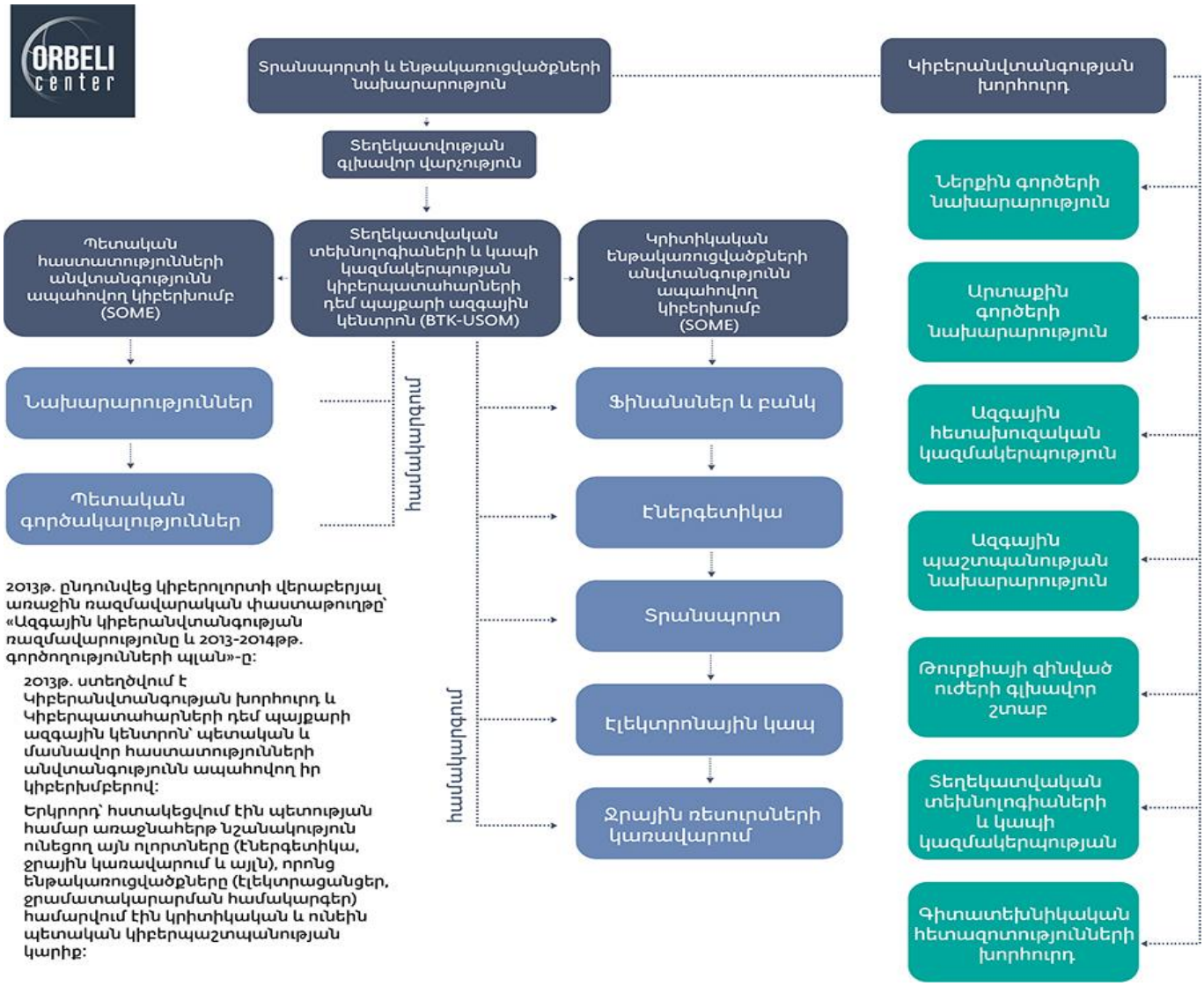
2013թ. ընդունվեց կիբերոլորտի վերաբերյալ առաջին ռազմավարական փաստաթուղթը՝ «Ազգային կիբերանվտանգության ռազմավարությունը և 2013-2014թթ. գործողությունների պլան»-ը, որը առավելապես վերաբերում էր ոլորտի անվտանգությունն ապահովող կառույցների ստեղծմանը[1]:

Արդյունքում 2013թ. ստեղծվում է Կիբերանվտանգության խորհուրդ և Կիբերպատահարների դեմ պայքարի ազգային կենտրոն՝ պետական և մասնավոր հաստատությունների անվտանգությունն ապահովող իր կիբերխմբերով: 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 կիբերպաշտպանության կարիք:

Մյուս կարևորագույն հարցերը էական նշանակություն ունեին ոլորտի հետագա զարգացումն ապահովելու տեսանկյունից: Հատկապես հրատապ էր համարվում անվտանգության մասնագետների պատրաստումը, ուսումնակրթական բազայի ստեղծումն ու ազգային կիբերտեխնոլոգիաների զարգացումը, միջազգային փոխգործակցությունը և այլն: Հարկ է նաև նշել, որ Թուրքիայի կառավարության 2012թ. հոկտեմբերին ընդունած որոշումով[2] կիբերանվտանգության 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-plani-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 փաստաթուղթը [3]: 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 տվյալների, 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 է[4]:

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 güvenlik 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 փոխտնօրեն Յ. Բաղրբաչքքի խոսքերով[5], Թուրքիան կիբերանվտանգության շուրջ 20.000 մասնագետների կարիք ունի: Այդ պատճառով կիբերկրթության 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: «Կիբերանվտանգություն» առարկան դասավանդվում է հիմնականում տեխնիկական գիտությունների բնագավառում կրթություն տրամադրող համալսարաններում **[Sevri, Topaloğlu, 2016; 928]**, նաև ռազմակրթական նշանակության որոշ ինստիտուտներում[7]:

Պետական հաստատությունների շարքում էական է Թուրքիայի գիտատեխնիկական հետազոտությունների խորհրդին կից գործող Կիբերանվտանգության ինստիտուտի դերը: Համակարգչային տեխնոլոգիաների տեխնիկական անվտանգությունն ապահովելու, կիբերսպառնալիքները 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 կիբերպաշտպանության վերապատրաստման դասընթաց»:

Այս քաղաքականությունից անմասն չի մնում նաև ռազմական ոլորտը, ինչի մասին վկայում է 2018թ. կիբերանվտագության ուսանողական մրցաշարին Թուրքիայի պաշտպանական արդյունաբերության գլխավոր վարչության քարտուղար Ի. Դեմիրի հայտարարությունը, որ Թուրքիան նպատակադրվել է առաջատար դիրքեր զբաղեցնել այս ոլորտում՝ ոչ միայն դիմակայելով կիբերհարձակումներին, 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 «Կիբերանվտանգության գործողությունների կենտրոնի» և «Կիբերանվտանգության ակադեմիայի» իր աշխատակիցների փորձառությունը:

[5] 20 bin siber güvenlik elemanına ihtiyaç var, https://www.trthaber.com/haber/turkiye/20-bin-siber-guvenlik-elemanina-ihtiyac-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, Կիբերանվտանգության 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 հրամանատարությունը[11]և 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: Միևնույն 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:

Օգտագործված գրականություն

Sevri, M., Topaloğlu, N. (2016). Türkiye'de siber güvenlik eğitiminin durumu. *International Conference on Education in Mathematics, Science & Technology (ICEMST),* s.928

Симаворян, А. (2018). Подходы к критическим инфраструктурам в Турции. *Глобус, 7 (96), 4-9.*

Հարությունյան, Գ., Մարջանյան, Ա., Վերանյան, Կ., Սիմավորյան, 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: