2
ՆՈՅԵՄԲԵՐԻ
2022

Luys Lույս®

ՊԱՏԵՐԱԶՄ ՎԱՐԵԼՈՒ ԿԻԲԵՌՄԻՋՈՑՆԵՐԻ ԻՐԱՎԱՉԱՓՈՒԹՅՈՒՆԸ ԵՎ ԿԻԲԵՌՊԱՇՏՊԱՆՈՒԹՅԱՆ ՈԼՈՐՏՈՒՄ ՀՀ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆԸ

ՊԱՏԵՐԱԶՄ ՎԱՐԵԼՈՒ ԿԻԲԵՌՄԻՋՈՑՆԵՐԻ ԻՐԱՎԱՉԱՓՈՒԹՅՈՒՆԸ ԵՎ ԿԻԲԵՌՊԱՇՏՊԱՆՈՒԹՅԱՆ ՈԼՈՐՏՈՒՄ ՀՀ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆԸ

ՆԵՐԱԾՈՒԹՅՈՒՆ

Պատմության ընթացքում աշխարհը բազմիցս ենթարկվել է հիմնովին փոփոխությունների՝ պայմանավորված տեխնոլոգիական զարգացման հետ: Ժամանակակից աշխարհում, մասնավորապես, 20-րդ դարի վերջին ինտերնետի ստեղծումը, ինչպես նաև դրան հաջորդած արհեստական բանականության ոլորտում տեղի ունեցող սրընթաց զարգացումները դարձել են կյանքի բոլոր բնագավառների վրա ազդելու ներուժ ունեցող հիմնական գործոնը: Տեխնոլոգիական զարգացման հիմնական միտումները շարունակական էական ազդեցություն են ունենում նաև զինված հակամարտությունների բնույթի վրա՝ ուրվագծելով պետությունների ռազմական առաջնահերթությունները: Զինված հակամարտությունները, դրանց կարգավորման կանոններն ու ռազմական գործը ոչ թե ստատիկ, այլ դինամիկ երևույթներ են, դրանք կտրված չեն գլոբալ համատեքստից և աշխարհում տեղի ունեցող փոփոխություններից: Զինված հակամարտությունները և գիտական-տեխնոլոգիական զարգացումը սերտորեն փոխկապակցված են: Այսպես, տեխնոլոգիական առաջընթացը փոփոխում է զինված հակամարտությունների բնույթը, իսկ զինված հակամարտությունների նոր բնույթով պայմանավորված պաշտպանության առաջնահերթություններն ու մարտահրավերները խթան են հանդիսանում տեխնոլոգիական առաջընթացի համար: Զարմանալի չէ, որ ռազմական փոխակերպմամբ վերաիմաստավորվեցին նաև զինված հակամարտությունների ֆիզիկական տիրույթի ավանդական ընկալումները: Այսօր արդեն կիբեռտիրույթը՝ օդային, ջրային և ցամաքային մարտադաշտերի հետ զուգահեռ լայնորեն ընկալվում և օգտագործվում է որպես այլընտրանքային մարտադաշտ, իսկ կիբեռզենքերը՝ սովորական զինատեսակներին զուգահեռ՝ որպես

պատերազմ վարելու այլընտրանքային միջոցներ: Այս ուղղությամբ վերջին մի քանի տասնամյակների ընթացքում տեղի ունեցող մշտական զարգացումները տրամաբանորեն հանգեցնում են միջազգային իրավական կարգավորումների նոր մեկնաբանությունների[1] և պաշտպանության ոլորտում պետական նոր առաջնահերթությունների ու հայեցակարգային մոտեցումների ձևավորմանը՝ դրանք առավել արդյունավետ կերպով հարմարեցնելու աշխարհում գերիշխող զինված հակամարտությունների նոր ձևերին: Այս համատեքստում հարկ է ընդգծել, որ կիբեռտիրույթում տեղի ունեցող փոփոխությունները թերևս առանձնանում են աննախադեպ արագությամբ՝ զգալի ազդեցություն ունենալով զինված հակամարտությունները վարելու տրամաբանության և պետական պաշտպանության կառավարման վրա: Զարմանալի չէ, որ կիբեռզենքերի մշակմանն ու զարգացմանը զուգընթաց՝ վերջին տասնամյակների ընթացքում միջազգային հանրությունը քննարկման առարկա է դարձրել նաև կիբեռզենքերի կիրառման իրավաչափության հարցը, կիբեռզենքերի կիրառման արդյունքում առաջացող մարտահրավերների իրավական կարգավորման հիմնախնդիրները և այն միջոցառումները, որոնք անհրաժեշտ է նախաձեռնել միջազգային և ներպետական մակարդակներով՝ համապատասխանաբար նվազեցնելու կիբեռզենքերի կիրառման արդյունքում հասցվող վնասն ու պետական պաշտպանության կազմակերպման համար մաքսիմալ օգտագործելու այն հնարավորությունները, որոնք ընձեռում է կիբեռզենքերի կիրառումը՝ պայմանավորված դրանց տեխնիկական բնութագրիչներով:

ԿԻԲԵՌԶԵՆՔԵՐԻ ԻՐԱՎԱՉԱՓՈՒԹՅԱՆ ՀԻՄՆԱԽՆԴԻՐԸ ՄԻՋԱԶԳԱՅԻՆ ԻՐԱՎՈՒՆՔԻ ՀԱՄԱՏԵՔՍՏՈՒՄ

Կիբեռտիրույթի և կիբեռզենքերի առանձնահատկությունները

Կիբեռզենքի կիրառման իրավաչափության և հնարավոր ազդեցության վերաբերյալ եզրակացություններ կայացնելու համար նախ անհրաժեշտ է անդրադառնալ դրանց էությանն ու զենքերի սովորական տեսակների համեմատությամբ հիմնական տարբերություններին:

[1] Այսպես, օրինակ, 1949 թվականի Ժնևի կոնվենցիաների 1952 թվականի մեկնաբանությունները 2016 թվականին փոփոխվել են նոր վերլուծություններով և պայմանագրային դրույթների նոր մեկնաբանություններով՝ չհաշված զինված հակամարտությունների նոր իրողություններին համապատասխանող այլ դոկտրինալ մեկնաբանությունները:

2022 թվականի ապրիլի դրությամբ ինտերնետի ակտիվ օգտատերերի թիվն աշխարհում, որոշ գնահատականների համաձայն, հասել է շուրջ 5 միլիարդի:[2] Կյանքի բոլոր բնագավառները մակրո և միկրո մակարդակներով զգալիորեն կառավարվում են ինտերնետի միջոցով: Հիմնական պետական ենթակառուցվածքների, ներառյալ՝ ռազմական ենթակառուցվածքների գործունեության կախվածությունը ինտերնետից ամբողջ աշխարհում օրեցօր ավելի էական է դառնում: Պետական պաշտպանության և անվտանգության համակարգերի գործունեությունը հաճախ գրեթե ամբողջությամբ հիմնված է տեղեկատվական տեխնոլոգիաների վրա: Այսպես, դեռ 2010 թվականին ԱՄՆ պետական հաղորդակցությունների շուրջ 98%-ը, որը տրամաբանորեն ներառում է նաև ռազմական բնագավառի հաղորդակցությունների զգալի մասը, իրականացվում էր քաղաքացիական բնույթի ինտերնետ ցանցերի միջոցով:[3]

Միևնույն ժամանակ, բազմաթիվ գործոններ կիբեռտարածքը դարձնում են գայթակղիչ ռազմական նպատակներով կիրառման տեսանկյունից: Կիբեռզենքերի ստեղծումը չի պահանջում մեծ ֆինանսական կամ մարդկային ռեսուրսներ և մատչելի է ցանկացած պետության: Միաժամանակ, պատերազմ վարելու նման միջոցներ կարող են ստեղծվել և կիրառվել նաև ցանկացած անհատի կամ խմբավորման կողմից՝ ինտերնետին և որևէ էլեկտրոնային սարքավորմանը հասանելիության պարագայում: Կիբեռզենքերը կարող են ստեղծվել կիրառման արդյունքում ինտենսիվության և ազդեցության տարաբնույթ հնարավորություններով՝ սկսած պատերազմ վարելու ոչ մահացու և ոչ կործանարար միջոցներից, որոնք թիրախային կերպով ներազդում են էլեկտրոնային համակարգերի վրա՝ առանց դրանց ֆիզիկապես վնաս հասցնելու, մինչև պոտենցիալ մահացու կամ ավերածություններ պատճառող պատերազմ վարելու միջոցները: Այսպիսով, հնարավոր է ստեղծել է կիբեռզենքերի լայն տեսականի: Միևնույն ժամանակ, կիբեռզենքի կիրառման հետևանքների լրջությունը պայմանավորված չէ դրանց կործանարար կամ մահաբեր պոտենցիալի աստիճանից՝ հաշվի առնելով կիբեռտարածքում պետական և մասնավոր համակարգերի, ռազմական,

[2] Statista Research Department, Jul. 7, 2022, https://www.statista.com/statistics/617136/digital-population-worldwide/

[3] Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks" (Texas Law Review Vol. 88, 2009-2010) p. 1542.

անվտանգային և քաղաքացիական ցանցերի փոխկապակցվածությունը: Այսպիսով, նույնիսկ պոտենցիալ կործանարար կամ մահաբեր ազդեցություն չունեցող կիբեռմիջոցները կարող են հանգեցնել պետական և սոցիալական կյանքի լայնամասշտաբ, էական և երկարատև խափանումների: Միևնույն ժամանակ, կիբեռմիջոցների կիրառմամբ իրականացվող հարձակումներն իրականացնող իրական սուբյեկտին շատ ավելի դժվար է հայտնաբերել, քան սովորական զինատեսակներով իրականացված հարձակման պարագայում հարձակումն իրականացնողին, ինչպես նաև շատ ավելի դժվար է ապացուցել համապատասխան հարձակմանը այս կամ այն պետության կամ խմբավորման վերագրելիությունը՝ պայմանավորված այն հանգամանքով, որ կիբեռտարածությունը չունի աշխարհագրական սահմաններ:[4] Հարկ է ընդգծել նաև, որ համաշխարհային ինտերնետ ցանցի իրավական կարգավորումները միջազգային և ներպետական մակարդակներով ավելի լիբերալ են և նվազ դետալացված, իսկ դրա նկատմամբ ինստիտուցիոնալ վերահսկողությունը ավելի թույլ՝ պայմանավորված կիբեռտիրույթի ֆիզիկական առանձնահատկություններով: Վերոհիշյալը դյուրին է դարձնում պատասխանատվությունից խուսափելու հնարավորությունները: Ստեղծված նոր իրողությունը թելադրում է, որ կիբեռպաշտպանությունն ու կիբեռանվտանգությունը պետությունների կողմից պետք է արժանանան բավարար ուշադրության: Ավելին, անհրաժեշտ է հաշվի առնել նաև այն հանգամանքը, որ կիբեռտիրույթը սերտորեն փոխկապակցված է օդային, ցամաքային և ջրային տիրույթների հետ՝ հաճախ զգալի ազդեցություն ունենալով ռազմական գործողությունների վրա պատերազմ վարելու այնպիսի միջոցների կիրառման արդյունքում, որոնք կառավարվում են համացանցով կամ վերահսկվում են էլեկտրոնային համակարգերի միջոցով: Պատահական չէ, որ պետությունները, որպես կանոն, դիտարկում են, կիբեռտարածքը որպես զինված հակամարտություններ վարելու առավել նպատակահարմար տիրույթ, իսկ կիբեռմիջոցների ռազմական նպատակներով օգտագործումը բարձրացնում է մի շարք տեսական իրավական և կիրառական հարցեր:

Պատերազմ վարելու նոր միջոցների մշակումն ու կիրառումը հաճախ սկզբնական ժամանակահատվածում բացասական է ընկալվում այն կանխավարկածով, որ նման զարգացումները ուղղված են լինելու պատերազմի

[4] Michael Robbat, “Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework and a Creation of a New Paradigm” (2000) B. U. J. Sci. & Tech. L. 264, 269.

ընթացքում տառապանքներն ու ավերածությունները մեծացնելուն՝ չնայած որոշ դեպքերում նոր ռամական տեխնոլոգիաների պատշաճ բարեխղճությամբ կիրառումը կարող է նույնիսկ նվազեցնել ավերիչ հետևանքները: Բնական է, որ ռազմական իրավունքի ոլորտում մասնագետները մեծ ուշադրություն են դարձնում նոր զենքերի կիրառման հնարավոր հետևանքների ու դրանց լույսի ներքո միջազգային իրավական կարգավորումների արդյունավետության վերլուծությանը: Որոշ դեպքերում նման վերլուծությունը կարող է հանգեցնել այս կամ այն նոր տեսակի զենքի ոչ իրավաչափության և, հետևաբար, դրա կիրառումը արգելող[5] կամ սահմանափակող իրավական կարգավորումների[6] ընդունման անհրաժեշտության մասին եզրահանգմանը: Իսկ որոշ դեպքերում նման վերլուծությունը կարող է հանգեցնել այն եզրահանգմանը, որ տվյալ զինատեսակը արգելող կամ սահմանափակող միջազգային իրավական կարգավորում ընդունելու անհրաժեշտությունը բացակայում է, կամ որ տվյալ զինատեսակի առանձնահատկությունները հաշվի առնող ճկուն մեկնաբանությունների կիրառման պարագայում առկա կարգավորումները բավարար են: Հենց այսպիսի մոտեցում է որդեգրվել միջազգային գիտական հանրության և պետությունների կողմից կիբեռզենքերի միջազգային-իրավական կարգավորման հարցում:[7]

Պատերազմ վարելու կիբեռմիջոցների իրավաչափությունը

Պատերազմ վարելու միջազգային հումանիտար իրավունքի (ՄՀԻ) կանոնները նպատակ ունեն հավասարակշռել ռազմական անհրաժեշտությունն ու մարդկության հիմնարար պահանջները:[8] 1899 թվականի ցամաքային պատերազմ վարելու օրենքների և սովորույթների մասին Հաագայի 2-րդ կոնվենցիայի նախաբանում առաջին անգամ ամրագրված, այսպես կոչված, Մարտենսի վերապահումը

---

[5] Այսպիսի մոտեցում է որդեգրվել, օրինակ, քիմիական և կենսաբանական զենքերի պարագայում Տես՝ «Մանրէաբանական (կենսաբանական) և թունավորող նյութեր պարունակող զենքի մշակման, արտադրության և կուտակման արգելման և դրա ոչնչացման մասին» 1972թ. կոնվենցիան, «Քիմիական զենքի մշակման, արտադրության, կուտակման, կիրառման արգելման և դրա ոչնչացման մասին» 1993թ. կոնվենցիան:

[6] Նման մոտեցում է որդեգրվել, օրինակ, հրկիզվող զենքերի պարագայում: Տես՝ «Որոշակի տեսակի սովորական զենքերի մասին, որոնք կարող են համարվել ավելորդ վնասվածքներ պատճառող կամ անընտրական ազդեցություն ունեցող» 1980թ. կոնվենցիայի (այսուհետ նաև՝ Որոշակի տեսակի սովորական զենքերի մասին կոնվենցիա) երրորդ արձանագրությամբ:

[7] Michael Schmitt et al, Tallinn Manual Applicable to International Law Applicable to Cyber Warfare (CUP 2013) 302 pages; Michael Schmitt et al, NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) 598 pages.

[8] Yves Sandoz et al, Commentary to the Additional Protocol I of the Geneva Conventions (1987) para.1389.

նախատեսում է, որ ՄՀԻ նորմերով չկարգավորվող դեպքերում «բնակչությունը և պատերազմող կողմերը գտնվում են միջազգային իրավունքի սկզբունքների պաշտպանության և գործողության ներքո, քանի որ դրանք բխում են քաղաքակիրթ ազգերի միջև հաստատված սովորույթներից, մարդասիրական օրենքներից և հասարակական գիտակցության պահանջներից»: Մարտենսի վերապահումը, այսպիսով, հանդես է գալիս որպես նվազագույն իրավական երաշխիք, որի հիմնական նպատակն է արմատավորել այն կանոնը, որ ՄՀԻ սովորութային բնույթ ունեցող նորմերի, մարդասիրության և հասարակական գիտակցության պահանջների ուժով ռազմական գործողությունների ընթացքում որոշ գործողություններ ոչ իրավաչափ են նույնիսկ այն պարագայում, երբ դրանք ուղղակիորեն արգելված չեն ՄՀԻ գրված կանոններով:[9] Եվ այս համատեքստում ՄՀԻ կարևորագույն դոգմատներից է հանդիսանում այն սովորութային բնույթ ունեցող կանոնը, որի համաձայն պատերազմող կողմերի իրավունքը պատերազմ վարելու միջոցների ընտրության հարցում անսահմանափակ չէ:[10]

Զենքի կիրառումը արգելելու կամ սահմանափակելու ՄՀԻ երկու հիմնական կառուցակարգերը

Ժամանակակից միջազգային իրավունքում առկա է զենքի կիրառումը արգելելու կամ սահմանափակելու երկու հիմնական կառուցակարգ՝ 1) ՄՀԻ ընդհանուր սկզբունքների միջոցով և 2) տվյալ զենքի կիրառումը արգելող կամ սահմանափակող միջազգային պայմանագրերի միջոցով:[11]

ՄՀԻ ընդհանուր սկզբունքները

Այսպես, ՄՀԻ ընդհանուր սկզբունքներից պատերազմ վարելու միջոցների իրավաչափության հարցի դիտարկման համար թերևս անկյունաքարային նշանակություն ունեն 1949 թվականի Ժնևի կոնվենցիայի 1977 թվականի 1-ին լրացուցիչ արձանագրությամբ ամրագրված (այսուհետ՝ 1-ին ԼԱ) տարբերակման սկզբունքը, որով արգելվում են պատերազմ վարելու per se (ինքնին) չտարբերակող

---

[9] A.P.V. Rogers, Law on the Battlefield (2004 MUP, 2nd edn.) 7.

[10] Տես՝ Ցամաքային պատերազմի օրենքների և սովորույթների մասին 1907թ. Հաագային կոնվենցիա, հոդ. 22, ինչպես նաև Միջազգային զինված ընդհարումների զոհերի պաշտպանության մասին 1949 թվականի օգոստոսի 12-ի ժնևի կոնվենցիաների 1977թվականի 1-ին լրացուցիչ արձանագրություն (1-ին ԼԱ), 35-րդ հոդվածի 1-ին մաս:

[11] A. Cassese, "Weapons Causing Unnecessary Suffering: are they Prohibited?" (1975) Rivista di diritto internazionale, 12.

(անընտրական) միջոցները և ավելորդ վնասվածքներ ու անհարկի տառապանքներ պատճառելու արգելքը, որի համաձայն ոչ իրավաչափ են պատերազմ վարելու բոլոր այն միջոցները, որոնք իրենց էությամբ պատճառում են ավելորդ վնասվածքներ և անհարկի տառապանքներ: Վերոհիշյալ ընդհանուր սկզբունքներն ունեն սովորութային բնույթ և պարտադիր են կիրառման համար ամբողջ միջազգային հանրության կողմից՝ անկախ այն հանգամանքից՝ արդյո՞ք պետությունը վավերացրել է 1-ին ԼԱ-ն, թե՞ ոչ:[12]

Այսպիսով, 1-ին ԼԱ շրջանակում կարգավորվում են պատերազմ վարելու բոլոր միջոցները, ներառյալ՝ արդեն փորձարկված և կիրառվող, նոր և ապագա զենքերը: Ցանկացած զենք ի սկզբանե պետք է ունենա այնպիսի չափանիշներ, որոնք հնարավոր կդարձնեն տվյալ զենքի կիրառումը վերոհիշյալ երկու սկզբունքներին համապատասխան:[13]

Տարբերակման սկզբունքը

Տարբերակման սկզբունքի հիմնական նպատակն է քաղաքացիական բնակչության և քաղաքացիական օբյեկտների պաշտպանությունը զինված հակամարտությունների ժամանակ, և այն բաղկացած է երկու հիմնական տարրերից՝ ա) քաղաքացիական անձանց և օբյեկտների վրա դիտավորությամբ իրականացված հարձակումների արգելք և բ) անընտրական հարձակումների արգելք:[14] 1-ին ԼԱ նորմերով անընտրական հարձակումներն են այն հարձակումները, որոնք, անկախ պատերազմ վարելու կիրառվող միջոցներից, ուղղված չեն կոնկրետ ռազմական օբյեկտների դեմ (օրինակ՝ հրթիռների, հրազենի կամ զրահատանկային սպառազինության անընտրական կիրառումը), ինչպես նաև per se անընտրական զինատեսակները:[15] Սույն վերլուծության համատեքստում

[12] Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law, Volume 1: Rules ("Customary IHL") Cambridge University Press 2005, 237-250.

[13] Տարբերակման սկզբունքը կարգավորված է նաև 1-ին ԼԱ 48-րդ և 51-րդ հոդվածներով, իսկ ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառելու արգելքը 1-ին ԼԱ 1-ին հոդվածի 2-րդ մասով և 35-րդ հոդվածի 2-րդ մասով: Քննարկվող սկզբունքների իրավական բովանդակությունը պատերազմ վարելու միջոցների իրավաչափության համատեքստում նաև մանրամասն վերլուծված է Միջուկային զենքի սպառնալիքի կամ օգտագործման իրավաչափության վերաբերյալ ՄԱԿ-ի միջազգային դատարանի խորհրդատվական կարծիքում (Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ (1996) para.78):

[14] Yoram Dinstein, The Conduct of Hostilities Under the Law of International Armed Conflict (2010 CUP, 2nd edn.) pp.124-128.

[15] 1-ին ԼԱ, 51-րդ հոդվածի 4-րդ մաս:

ցանկացած զենքի, այդ թվում՝ կիբեռզենքերի իրավաչափության տեսանկյունից առավել հետաքրքրություն է ներկայացնում հենց ինքին անընտրական զենքերի կիրառման արգելքը: 1-ին ԼԱ-ն ինքին անընտրական զինատեսակներով անընտրական հարձակումները սահմանում է որպես՝

- պատերազմ վարելու այնպիսի միջոցների կամ մեթոդների կիրառմամբ իրականացվող հարձակումներ, որոնք չեն կարող ուղղված լինել ռազմական կոնկրետ օբյեկտների դեմ, կամ՝
- հարձակումներ, որոնք իրականացվում են պատերազմ վարելու այնպիսի մեթոդներով կամ միջոցներով, որոնց հետևանքները ինքին չեն կարող սահմանափակվել, ինչպես դա պահանջվում է 1-ին ԼԱ կանոնների համապատասխան և որոնք յուրաքանչյուր դեպքում վնաս են հասցնում ռազմական և քաղաքացիական օբյեկտներին, կոմբատանտներին և քաղաքացիական անձանց՝ առանց տարբերակման:[16]

Տարբերակման սկզբունքն ամրագրող միջազգային իրավական կարգավորումներն ակնհայտորեն ընդարձակ և վերացական են իրենց բնույթով, և վերոհիշյալ դրույթների տառացի մեկնաբանության պարագայում կարելի է եզրահանգել, որ պատերազմ վարելու միակ միջոցը, որն իր էությամբ և պարամետրներով կարող է դիտարկվել որպես ինքին անընտրական՝ կենսաբանական զենքն է, որի կիրառման արդյունքում հետևանքները չեն կարող սահմանափակվել, ինչպես դա պահանջվում է 1-ին ԼԱ կանոններով: Մինչդեռ գոյություն ունեցող մյուս բոլոր զենքերը, որոնք առաջին հայացքից կարող են ընկալվել որպես ոչ ընտրական, իրականում ոչ թե per se անընտրական են, այլ ունեն ոչ ընտրական եղանակով կամ տարբերակման սկզբունքի խախտմամբ կիրառվելու մեծ ներուժ: Անընտրական կիրառման ներուժն ու մեծ հավանականությունը, սակայն, չեն դարձնում այս կամ այն զինատեսակը ոչ իրավաչափ՝ 1-ին ԼԱ իմաստով: Հարձակումների ոչ ընտրական բնույթը ավելի հաճախ պայմանավորված է լինում որոշակի իրավաչափ զենքերի կիրառման եղանակներով և ոչ թե զենքի տարբերակման սկզբունքին համապատասխան կիրառելը անհնարին դարձնող տեխնիկական բնութագրիչներով:

[16] 1-ին ԼԱ, հոդված 51 մաս 4:

Ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառելու արգելքը

Ի տարբերություն տարբերակման սկզբունքի՝ ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառելու արգելքն ուղղված է կոմբատանտների նվազագույն պաշտպանությանը այնպիսի վնասվածքներից կամ տառապանքներից, որոնք անհրաժեշտ չեն ռազմական առավելություն ստանալու համար, կամ որոնք պատճառելը չի բխում ռազմական անհրաժեշտությունից: Հիշյալ սկզբունքի համաձայն՝ ոչ իրավաչափ են պատերազմ վարելու բոլոր այն միջոցներն ու մեթոդները, որոնք ինքին՝ իրենց տեխնիկական պարամետրերով պայմանավորված կոմբատանտներին պատճառում են ավելորդ վնասվածքներ և անհարկի տառապանքներ[17]: Այսպիսով, թե՛ տարբերակման սկզբունքի, թե՛ ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառելու արգելքի պարագայում ՄՀԻ-ով զենքի ինքնին իրավաչափությունը որոշելու համար կարևորվում են զենքի տեխնիկական բնութագրիչները:

Զենքի կիրառումը արգելելուն կամ սահմանափակելուն ուղղված միջազգային պայմանագրերը

ՄՀԻ ընդհանուր սկզբունքների հետ մեկտեղ միջազգային իրավունքում ընդունված է նաև զենքի կիրառումը արգելելուն կամ սահմանափակելուն ուղղված միջազգային պայմանագրերի ընդունումը:[18] Ի տարբերություն ՄՀԻ ընդհանուր սկզբունքների՝ միջազգային պայմանագրերով սահմանվում է արգելք կամ սահմանափակում կոնկրետ զենքերի կամ զենքերի կատեգորիաների վրա: Ընդ որում, պայմանագրային դրույթներն ունեն պարտադիր ուժ այն պետությունների

---

[17] Ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառող զենքի օրինակ է ցանկացած զենք, որի առաջնային ազդեցությունը մարդու մարմնում ռենտգենային ճառագայթների միջոցով չհայտնաբերվող բեկորներով վնասելն է: Պատերազմ վարելու այդպիսի միջոցները արգելված են Որոշակի տեսակի սովորական զենքերի մասին կոնվենցիայի առաջին արձանագրությամբ հենց այն տրամաբանությամբ, որ բեկորների հայտնաբերման անհնարինությունն արդեն իսկ hors de combat կոմբատանտների մոտ չի կարող դիտարկվել որպես անհրաժեշտ ռազմական առավելություն ստանալու նպատակ հետապնդող:

[18] Տե՛ս, օրինակ, «Մանրէաբանական (կենսաբանական) և թունավորող նյութեր պարունակող զենքի մշակման, արտադրության և կուտակման արգելման և դրա ոչնչացման մասին» 1972թ. կոնվենցիան, «Քիմիական զենքի մշակման, արտադրության, կուտակման, կիրառման արգելման և դրա ոչնչացման մասին» 1993թ. կոնվենցիան, Որոշակի տեսակի սովորական զենքերի մասին կոնվենցիան, «Հակահետևակային ականների օգտագործումը, պաշարների կուտակումը, արտադրությունը և փոխանցումն արգելելու և դրանք ոչնչացնելու մասին» 1997թ. կոնվենցիան, «Կասետային զինամթերքի մասին» 2008թ. կոնվենցիան և այլն:

համար, որոնք միացել են համապատասխան պայմանագրին, բացառությամբ այն դեպքերի, երբ պայմանագրային որոշակի դրույթներ ունեն սովորութային բնույթ՝ պարտադիր բնույթ ունենալով բոլոր պետությունների համար:

Զենքի կիրառումը արգելելու կամ սահմանափակելու ՄՀԻ հիմնական կառուցակարգերի վերաբերյալ եզրահանգումը

Հարկ է ընդգծել, որ զենքի կիրառումը արգելելու կամ սահմանափակելու երկու հիմնական կառուցակարգերը փոխլրացնող են: Այսպես, մի կողմից ՄՀԻ ընդհանուր սկզբունքները վերացական ձևակերպումների և տառացի մեկնաբանության արդյունքում փաստացի կարող են հիմք հանդիսանալ արգելելու շատ սահմանափակ տեսակի զենքեր, ինչի պատճառով հաճախ դիտարկվում են որպես պատերազմ վարելու մեթոդների և միջոցների կարգավորման ոչ արդյունավետ կառուցակարգ: Մյուս կողմից՝ հենց ՄՀԻ ընդհանուր սկզբունքներն են սովորաբար խթան հանդիսանում այս կամ այն զենքի պայմանագրային կարգավորման համար:

Ցանկացած զենք կարող է լինել.

ա) ոչ իրավաչափ այն պատճառով, որ ինքնին՝ պայմանավորված իր բնութագրիչներով, չի կարող կիրառվել ՄՀԻ հիմնարար սկզբունքներին համապատասխան, մասնավորապես տարբերակման սկզբունքին և ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառելու արգելքի սկզբունքին,

բ) ոչ իրավաչափ՝ միջազգային պայմանագրային կարգավորման արդյունքում, կամ՝

գ) *per se* իրավաչափ, սակայն ՄՀԻ հիմնարար սկզբունքների խախտմամբ կիրառվելու մեծ հավանականությամբ և ներուժով:[19]

[19] David Turns, “Weapons in the ICRC Study on Customary International Humanitarian Law” (2006) J. Conflict and Sec.L. 208.

Կիբեռզենքերի կիրառման հնարավոր հետևանքներն ու հիմնական իրավական հարցերը

Պատերազմ վարելու կիբեռմիջոցները կարող են օգտագործվել կիբեռհարձակման, կիբեռպաշտպանության և կիբեռզսպման եղանակով միջազգային կամ ոչ միջազգային զինված հակամարտության համատեքստում ռազմական նպատակներին հասնելու համար: Պատերազմ վարելու կիբեռմիջոցները կարող են օգտագործվել տարբեր եղանակներով, օրինակ՝ որոշակի ռազմական օբյեկտների չեզոքացում, տեղեկատվության մանիպուլյացիաներ և ձևափոխում որոշակի ռազմական նպատակին հասնելու համար, կիբեռհարձակում, կիբեռհետախուզություն և այլն:[20] Կիբեռմիջոցները կարող են կիրառվել քաղաքացիական բնակչության շրջանում խուճապ առաջացնելու, ռազմական առավելություն ձեռք բերելուն նպաստելու, ներառյալ՝ որոշակի համակարգերի գործունեությունը խաթարելու կամ մարդկանց կամ առարկաներին ֆիզիկական վնաս և ավերածություններ պատճառելու միջոցով: Կիբեռզենքերի կիրառումը պատերազմական իրավիճակներում և այդպիսի իրավիճակներից դուրս վերջին տասնամյակների ընթացքում բազմիցս է կիրառվել: Առավել մեծ հնչեղություն ստացված օրինակներն էին Էստոնիայի նկատմամբ 2007 թվականին իրականացված կիբեռօպերացիան, որն իրականացվել էր խաղաղ պայմաններում՝ միջազգային և ոչ միջազգային զինված հակամարտության համատեքստից դուրս, և որի վերագրելիությունը որևէ պետությանը ապացուցված չէ, ռուս-վրացական զինված հակամարտության ընթացքում տեղի ունեցած գործողությունները, իրանական միջուկային ցենտրիֆուգները վնասելու համար օգտագործվող «Սթաքսնեթ» որդի կիրառումը, կինետիկ հարձակումներին զուգահեռ՝ կիբեռզենքերի կիրառումը Սիրիայում: Հարկ է նաև ընդգծել, որ պետությունների կողմից կիբեռզենքերի պոտենցիալ կիրառման հնարավորության մասին են վկայում նաև, inter alia, կիբեռպաշտպանության և կիբեռանվտանգության ռազմավարությունները: Պատահական չէ, որ վերջին տասնամյակներում կիբեռզենքերի կիրառման միջազգային իրավական կարգավորման բազմաթիվ խնդիրներ հանդիսանում են ակադեմիական դեբատների և քննարկումների առարկա: Իրավական տեսանկյունից, մասնավորապես, ծագում են հետևյալ հարցերը. որ կիբեռգործողությունները կարող են որակվել որպես հարձակում 1-ին

[20] Lt Col Lionel D. Alford, Jr., USAF, Cyber Warfare: Protecting Military Systems (Tutorial), HSDL 2000, p. 105 at: file:///Users/Apple/Downloads/442130.pdf; Royal Danish Defence College, Joint Doctrine for Military Cyberspace Operations (Copenhagen, Sept. 2019) p.25.

լրացուցիչ արձանագրության իմաստով և արդյո՞ք կիբեռգործողության արդյունքում ֆիզիկական կամ կինետիկ հետևանքները նախապայման են գործողությունը որպես հարձակում որակելու համար, որ կիբեռօպերացիաները կարող են ինքնին որակվել որպես միջազգային կամ ոչ միջազգային զինված հակամարտություն, արդյո՞ք ռազմական էլեկտրոնային տվյալները համարվում են ռազմական օբյեկտ, թե՞ ոչ և բազմաթիվ այլ հարցադրումներ: Սակայն այս բոլոր հարցադրումներն իրականում կիբեռզենքերի կիրառման միջազգային իրավական կարգավորումների դետալներ են ընդամենը, որոնք պարբերաբար քննարկվում են գիտնականների և ՄՀԻ փորձագետների կողմից և որոնց վերաբերյալ միասնական կարծիքը գիտական շրջանակներում բացակայում է, իսկ մեկնաբանությունները ժամանակի ընթացքում հաճախ ենթարկվում են փոփոխությունների: Միևնույն ժամանակ, հարկ է ընդգծել, որ ոլորտի փորձագետները միակարծիք են այն մասին, որ կիբեռզենքերի կիրառումն իրավաչափ է ՄՀԻ տեսանկյունից:

Կիբեռզենքերի իրավաչափությունը միջազգային պայմանագրերով և ՄՀԻ ընդհանուր սկզբունքներով

Կիբեռզենքերի իրավաչափությունը որոշելու համար անհրաժեշտ է որոշել, թե արդյո՞ք կիբեռզենքերի կիրառումը՝

1) արգելված կամ սահմանափակված է որևէ միջազգային պայմանագրով,
2) հնարավոր է ՄՀԻ ընդհանուր սկզբունքներին համապատասխան:

<u>Կիբեռզենքերի իրավաչափությունը միջազգային պայմանագրերով</u>

Ինչ վերաբերում է պայմանագրային կարգավորմանը, ապա հարկ է ընդգծել, որ որևէ միջազգային պայմանագրով այսօր կիբեռզենքերի կիրառումը արգելված չէ, չկան նաև միջազգային պայմանագրեր ուղղված կիբեռզենքերի կիրառման սահմանափակմանը կամ կարգավորմանը: Միջազգային պայմանագրով կիբեռզենքերի կարգավորման բացակայությունը տրամաբանական է՝ հաշվի առնելով կիբեռմիջոցների բնույթն ու նոր տեսակի միջոցների ստեղծման սրընթաց տեմպերը, ինչի արդյունքում ցանկացած պայմանագիր արդեն մշակման փուլում կարող է դառնալ ոչ արդիական և հետևապես՝ ոչ արդյունավետ: Միջազգային պայմանագրի մշակումը նպատակահարմար չէ նաև այն պատճառով, որ նման միջազգային պայմանագիրը կիրառման համար պարտադիր կլինի միայն

պետությունների համար՝ ստեղծելով ավելի բարենպաստ պայմաններ կազմակերպված զինված խմբերի համար:

Կիբեռզենքերի իրավաչափությունը ՄՀԻ ընդհանուր սկզբունքներով

Այսպիսով, հաջորդ թեսթը ՄՀԻ ընդհանուր սկզբունքներին համապատասխան կիբեռզենքերի կիրառման հնարավոր լինելու հարցն է: Ընդ որում, որպես ելակետային է դիտարկվում այն պնդումը, որ կիբեռմիջոցների կիրառումը կարգավորվում է ՄՀԻ նորմերով և պետք է իրականացվի ՄՀԻ հիմնարար սկզբունքներին համապատասխան բոլոր այն դեպքերում, երբ կիբեռմիջոցներով գործողությունն իրականացվում է միջազգային կամ ոչ միջազգային զինված հակամարտության համատեքստում և բավարարում է 1-ին լրացուցիչ արձանագրության 49-րդ հոդվածի 1-ին մասով սահմանված հարձակման պահանջներին[21] կամ ինքնին կարող է որակվել որպես միջազգային կամ ոչ միջազգային զինված հակամարտություն:

ա) Կիբեռզենքերի կիրառումը դիտավորությամբ ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառելու արգելքի համատեքստում

Թեև տեսականորեն հնարավոր է կիբեռմիջոցների կիրառումը դիտավորությամբ ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառելու համար, սակայն ինքնին դրանց իրավաչափությունը ավելորդ վնասվածքներ և անհարկի տառապանքներ պատճառելու արգելքի համատեքստում հարցեր չի առաջացնում: Ավելին, կա կարծիք, որ կիբեռզենքերն ունեն ամենամեծ ներուժը նվազագույնին հասցնելու վնասվածքներն ու տառապանքները:[22]

բ) Կիբեռզենքերի կիրառումը տարբերակման սկզբունքի համատեքստում

Առավել խնդրահարույց է համարվում կիբեռզենքերի կիրառումը տարբերակման սկզբունքի համատեքստում:

[21] 1-ին ԼԱ 49-րդ հոդվածի 1-ին մասի համաձայն. «Հարձակումներ նշանակում են հակառակորդի նկատմամբ ճնշման գործողությունները, անկախ այն բանից, դրանք կատարվում են հարձակման, թե պաշտպանության ժամանակ»:

[22] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations" (2012, NATO CCD COE Publications) 91, 104.

Համեմատած ավանդական զենքերի հետ՝ պատերազմ վարելու կիբեռմիջոցները մեծ հավանականությամբ կարող են օգտագործվել տարբերակման սկզբունքի խախտմամբ, որը պայմանավորված է երկու հիմնական գործոնով.

1. Նույնիսկ եթե կիբեռօպերացիան ծրագրված է կոնկրետ ռազմական օբյեկտի դեմ, կիբեռտարածքում ռազմական և քաղաքացիական ենթակառուցվածքների փոխկապակցվածության աննախադեպ աստիճանը կարող է հանգեցնել վնասակար ծրագրերի անկանխատեսելի և ոչ միտումնավոր ներթափանցման քաղաքացիական ցանցեր:
2. Մի կողմից՝ ասիմետրիկ պատերազմներ վարելու ժամանակակից միտումներն ու պատերազմ վարելու կիբեռմիջոցների հեշտ հասանելիությունը ցանկացած անհատների, խմբավորումների և պետությունների համար և մյուս կողմից՝կիբեռգործողության իրականացման աղբյուրը և կիբեռգործողության վերագրելիությունը պարզելու խոչընդոտները՝ պայմանավորված կիբեռմիջոցների առանձնահատկություններով, դարձնում են կիբեռմիջոցների ոչ ընտրական կիրառումը շատ գրավիչ՝ համապատասխան քաղաքական նպատակների հասնելու և որոշակի սուբյեկտների իրենց քաղաքական կամքը թելադրելու նպատակով:

Զարմանալի չէ, որ կիբեռզենքերը գործնականում հաճախ համեմատվում են զանգվածային ոչնչացման զենքերի հետ:[23]

Այստեղ հարկ է ընդգծել, որ կիբեռօպերացիաները, որոնք չեն բավարարում «հարձակում» եզրույթի հիմնական չափորոշիչներին, բայց իրականացվում են զինված հակամարտության համատեքստում, նույնպես որոշ չափով կարգավորվում են ՄՀԻ տարբերակման սկզբունքով: Զինված հակամարտությունները, որպես կանոն, ստեղծում են բազմաթիվ վտանգներ քաղաքացիական բնակչության համար, իսկ տարբերակման սկզբունքի հիմնական նպատակն է այդ վտանգները նվազագույնին հասցնելը:[24] Հենց այս տրամաբանությամբ 1-ին լրացուցիչ

[23] Տե՛ս, օրինակ, Benjamin Hatch, "Defining A Class Of Cyber Weapons As WMD: An Examination Of The Merits", Journal Of Strategic Security 11, No.1 (2018) pp.43-61; Patrick Cirenza, An Evaluation of the Analogy Between Nuclear and Cyber Deterrence, Advisors: Professor Coit D. Blacker and Phillip Taubman, Center for International Security and Cooperation Freeman Spogli Institute for International Studies Stanford University June 2015 at: https://stacks.stanford.edu/file/druid:sh530vk4641/An%20Evaluation%20of%20the%20Analogy%20Between%20Nuclear%20and%20Cyber%20Deterrence.pdf; Scott Shackelford, “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law” (Berkeley J. Int'l Law, 2009) և այլն:

[24] Yves Sandoz et al, supra n. 8, para.1935

արձանագրության 51-րդ հոդվածի 1-ին մասի համաձայն. «Քաղաքացիական բնակչությունը և քաղաքացիական առանձին անձինք օգտվում են *ռազմական օպերացիաների* [մեր ընդգծումն է] կապակցությամբ առաջացած վտանգների ընդհանուր պաշտպանությունից»: Վերոհիշյալ ձևակերպումից ակնհայտ է, որ «ռազմական օպերացիա» եզրույթը ավելի լայն է, քան «հարձակում» եզրույթը 1-ին լրացուցիչ արձանագրության համատեքստում, և վկայում է այն մասին, որ քաղաքացիական անձինք օգտվում են ՄՀԻ դրույթների պաշտպանությունից և տարբերակման սկզբունքը կիրառելի է ոչ միայն հարձակումների ժամանակ, այլ նաև ցանկացած ռազմական օպերացիայի համատեքստում, թեև տարբերակման սկզբունքն ամրագրող մյուս բոլոր դրույթներով ամրագրվում է հարձակումների ընթացքում քաղաքացիական բնակչության պաշտպանությունը:[25] Ամփոփելով՝ կարելի է եզրահանգել, որ քաղաքացիական բնակչությունն օգտվում է ռազմական գործողությունների ընթացքում ընդհանուր պաշտպանությունից, մինչդեռ պաշտպանության հստակ երաշխիքները սահմանվում են հենց հարձակումների ընթացքում:

Հաշվի առնելով կիբեռտարածության մեջ քաղաքացիական, մասնավոր և ռազմական համակարգերի մեծ փոխկապակցվածությունը և կիբեռզենքերի կիրառման հետևանքների վերահսկման դժվարությունը՝ որոշ հեղինակներ տարակուսելի են համարում կիբեռհարձակումներով ճշգրիտ թիրախավորելու հնարավորությունը:[26] Կիբեռհարձակումների ժամանակ ռազմադաշտ է համարվում կիբեռտարածքը, որը նկարագրվում է որպես «բոլորին ամեն ինչի հետ կապող» ցանց,[27] «համակարգիչների և հեռահաղորդակցության միջոցով մարդկանց գլոբալ փոխկապակցվածություն, որը հաշվի չի առնում ֆիզիկական աշխարհագրական գործոնները»[28] կամ «տեղեկության և մարդկանց միջև հարաբերակցման վիրտուալ միջավայր»[29]: ԱՄՆ նախագահական դիրեկտիվում կիբեռտարածքը սահմանվում է որպես տեղեկատվական-տեխնոլոգիական ենթակառուցվածքների

[25] 1-ին ԼԱ, 51-րդ հոդվածի 2-րդ մաս, 51-րդ հոդվածի 4-րդ մաս, 52-րդ հոդվածի 1-ին մաս, 52-րդ հոդվածի 2-րդ մաս:
[26] Bradley Graham, "Cyberwar: A New Weapon Awaits a Set of Rules; Military, Spy Agencies Struggle to Define Computers' Place in U.S. Arsenal" (citing A.Cebrowski) (08.07.1988) Wash.Post, Al. at: http://cryptome.org/jya/cyber-how.htm.
[27] Noam Lubell, "Cyber Warfare as Armed Conflict" at Bruges Colloquium "Technological Challenges for the Humanitarian Legal Framework" (CICR 41, 2010) 43.
[28] Steven Hildreth, CRS Report for Congress on Cyberspace (2001) 1 (footnote 1).
[29] USA Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure, 1.

փոխկապակցված և միմյանցից կախված ցանց, որը ներառում է ինտերնետը, տեղեկատվական հաղորդակցման ցանցերը, համակարգչային համակարգերը, ներկառուցված պրոցեսորներն ու կարգավորիչները:[30]

Կիբեռհարձակումները, որպես կանոն, ուղղված են լինում ցանցային համակարգչային համակարգերի դեմ՝ նպատակ ունենալով՝

1) շարքից հանել կամ վնասել համապատասխան համակարգչային համակարգը (օրինակ՝ պետական կայքերի աշխատանքի ժամանակավոր խափանումը),

2) մանիպուլացնել, աղավաղել, փոխել կամ ոչնչացնել որոշակի տեղեկություններ (օրինակ՝ ռազմական նշանակության տեղեկությունների կամ առցանց փոխանցվող հրամանների ոչնչացումը),

3) մանիպուլացնել, աղավաղել, փոխել կամ ոչնչացնել տեղեկություններ, որոնք անհրաժեշտ են որևէ սկզբնական թիրախ հանդիսացող օբյեկտի բնականոն գործունեությունը խափանելու համար (օրինակ՝ ռազմական օդային ուժերի համապատասխան օբյեկտները): [31]

Որոշ փորձագետների կարծիքով, համակարգի կոնկրետ մասի նկատմամբ ցանկացած հարձակում պետք է դիտարկվի որպես ամբողջ համակարգի դեմ հարձակում,[32] ինչն առերևույթ վկայում է այն մասին, որ նույնիսկ այն կիբեռհարձակումները, որոնք ծրագրված են կոնկրետ ռազմական օբյեկտը թիրախավորելու համար, ավելի հավանական է, որ բացասական հետևանքները տարածեն նաև քաղաքացիական անձանց և քաղաքացիական օբյեկտների վրա բոլոր այն դեպքերում, երբ վերջիններս որևէ կերպ փոխկապակցված են վիրտուալ տարածության մեջ թիրախ հանդիսացող օբյեկտի հետ:[33] Եվ յուրաքանչյուր նման դեպքում ծագում է իրականացված հարձակման ՄՀԻ տարբերակման և համաչափության սկզբունքներին համապատասխանության հարցը: Այսպիսով, կիբեռզենքերի կիրառման հիմնական խնդիրը կայանում է նշված զենքերով

[30] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD - 54/HSPD23); USA Cyberspace Policy Review, supra n. 29, 1.
[31] Michael N. Schmitt (Editor-in-Chief) et. al., *Blue Book* (89 INT'L L. STUD. 2013) Noam Lubell, "Lawful Targets In Cyber Operations: Does The Principle Of Distinction Apply?", 255.
[32] Scott Shackelford, supra n. 23, 200-201.
[33] Nils Melzer, "Cyber Operations and Jus in Bello" Disarmament Forum (2011) 10.

իրականացված հարձակման հետևանքների հաշվարկման և մոդելավորման բարդության մեջ: Միևնույն ժամանակ կարևոր է ընդգծել, որ չնայած ոչ ընտրական կիրառման մեծ ներուժի, բարեխիղճ և արհեստավարժ ծրագրման և իրականացման պարագայում պատերազմ վարելու կիբեռմիջոցները կարող են լինել ճշգրիտ կոնկրետ ռազմական օբյեկտը թիրախավորելու համար՝ համապատասխանելով ՄՀԻ տարբերակման սկզբունքի պահանջներին: Ավելին, կիբեռզենքերի կիրառումը կարող է հնարավորություն ընձեռնել թիրախավորել այնպիսի օբյեկտներ, որոնց ֆիզիկական թիրախավորումը ավանդական զինատեսակով այլ հավասար պայմաններում կարող էր հանգեցնել համաչափության սկզբունքի խախտման և անհամաչափ վնասների քաղաքացիական անձանց և օբյեկտների շրջանում, ոչ համաչափ հարձակման (օրինակ, ռազմական տվյալների բազաների ֆիզիկական ոչնչացումը որոշակի հանգամանքների պարագայում): Կարելի է մտածել զինված հակամարտությունների համատեքստում և այդպիսի համատեքստից դուրս կիբեռմիջոցների կիրառման բազմաթիվ սցենարներ: Այսպես, անընտրական եղանակով կիբեռզենքերը կարող են օգտագործվել, օրինակ, առողջապահական համակարգը թիրախավորելով՝ նախնական բժշկական տվյալների և գրառումների փոփոխման միջոցով կամ էլեկտրոնային առողջապահական համակարգերը վնասելու միջոցով, ինչը կարող է հանգեցնել հսկայական վնասների և նույնիսկ վտանգ հանդիսանալ քաղաքացիական բնակչության կյանքի և առողջության համար: Կիբեռմիջոցները կարող են օգտագործվել անընտրական եղանակով՝ թիրախավորելու համար տվյալ պետության բանկային համակարգը, և կախված համապատասխան կիբեռգործողության մասշտաբից, տևողությունից և ինտենսիվությունից՝ նման գործողությունը կարող է առաջացնել տագնապ քաղաքացիական բնակչության շրջանում և իր հետևանքներով կարող է նույնիսկ հասնել այն շեմին, որը կարող է դիտարկվել որպես քաղաքացիական բնակչության ահաբեկում (ինչն ինքնին արգելված է ՄՀԻ հիմնարար դրույթներով[34])՝ առանց զգալի ֆիզիկական վնաս պատճառելու մարդկանց կամ օբյեկտներին: Կիբեռմիջոցներն ունեն ներուժ թիրախավորելու գրեթե ցանկացած ենթակառուցվածք՝ սկսած էլեկտրակայաններից, նավթի կամ գազի խողովակներից և քիմիական գործարաններից, վերջացրած ջրի կամ էլեկտրաէներգիայի մատակարարումով՝ պայմանավորված նման ենթակառուցվածքների ցանցային բնույթով և դրանց գործարկման համար համացանցից մեծ կախվածությամբ:

[34] 1-ին ԼԱ, 51-րդ հոդվածի 2-րդ մաս; Jean-Marie Henckaerts and Louise Doswald-Beck, supra n.12, rule 2.

Կիբեռմիջոցները կարող են կիրառվել ավիացիոն կամ ծովային համակարգերը խափանելու համար՝ առաջացնելով քաոս և ավերածություններ, պատճառ դառնալով քաղաքացիական բնակչության շրջանում կորուստների, կամ կարող են օգտագործվել շարքից հանելու լուսացույցները՝ առաջացնելով ճանապարհատրանսպորտային պատահարներ և պատճառելով զգալի ֆիզիկական վնաս քաղաքացիական բնակչությանն ու օբյեկտներին: Միևնույն ժամանակ, կիբեռզենքերի անընտրական կիրառման հետ մեկտեղ դրանք կարող են կիրառվել նաև իրավաչափորեն և ճշգրիտ կերպով թիրախավորելու կոնկրետ ռազմական օբյեկտներ կամ փոխելու ռազմական ցանցերի միջոցով փոխանցվող հրամանատարության կամ հսկողության ցուցումները կամ տեղեկությունները՝ հակառակորդի ռազմական գործողությունների վրա ազդելուկամ որոշակի ռազմական օբյեկտ ֆիզիկապես շարքից հանելու նպատակով. օրինակ՝ որևէ համակարգի կամ օբյեկտի բնականոն գործունեության համար նախադրյալ հանդիսացող տվյալների փոփոխում իրականացնելով և այդպիսով մանիպուլացնելով ու խափանելով դրա բնականոն գործարկումը (օրինակ՝ փոխելով օպտիմալ ջերմաստիճանի ռեժիմը կամ որոշակի նյութի արագությունն ու ուղղությունը), որը միտված է հանգեցնելու թիրախավորված օբյեկտի ֆիզիկական վնասման: Այսպիսով, տեխնիկական փորձագետների կարծիքով՝ պատշաճ ջանասիրության դրսևորման պարագայում կարող են կիրառվել ՄՀԻ հիմնարար սկզբունքներին, մասնավորապես՝ տարբերակման սկզբունքին համապատասխան:[35]

Եվ չնայած այն հանգամանքին, որ կիբեռզենքերն ունեն անընտրական կերպով օգտագործվելու մեծ ներուժ և հավանականություն, ընդհանուր առմամբ պատերազմ վարելու կիբեռմիջոցները չեն կարող դիտարկվել որպես per se անընտրական և ոչ իրավաչափ, և համարվում են պատերազմ վարելու իրավաչափ միջոցներ: Ինչպես և ցանկացած այլ զինատեսակ պատերազմ վարելու կիբեռմիջոցները պետք է կիրառվեն ՄՀԻ հիմնարար սկզբունքներին, ներառյալ՝ տարբերակման սկզբունքին, համապատասխան՝ տարբերակելով քաղաքացիական անձանց կոմբատանտներից և հարձակման իրավաչափ օբյեկտ հանդիսացող անձանցից, քաղաքացիական օբյեկտները ռազմական օբյեկտներից:[36] Ընդ որում, կարևոր է ընդգծել, որ նույնիսկ

[35] Robin Geiss, "The Legal Regulation of Cyber Attacks in Times of Armed Conflict" Bruges Colloquium (2010) CIRC, 51; Jeffrey Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the age of Cyber Warfare" (2007-2008) Mich.L.Rev. 1434.
[36] Tallinn Manual, supra n. 7, p. 95, rule 31; 1-ին ԼԱ, 48-րդ հոդված, 51-րդ հոդվածի 2-րդ մաս; Henckaerts and Doswald-Beck, supra n.12, 3.

զինված հակամարտության համատեքստում որոշ տեսակի հոգեբանական օպերացիաների և, մասնավորապես, քարոզչության պարագայում քաղաքացիական բնակչության թիրախավորումը իրավաչափ է, իսկ ՄՀԻ տարբերակման սկզբունքը կիրառելի չէ:[37]

Կիբեռզենքերի կիրառման իրավաչափության վերաբերյալ եզրահանգումը

Այսպիսով, վերոհիշյալ վերլուծությունից կարելի է ամփոփել, որ ՄՀԻ տեսանկյունից կիբեռմիջոցների կիրառումը զինված հակամարտությունների ընթացքում իրավաչափ է, դրանց կիրառումը կարգավորվում է ՄՀԻ նորմերով, և կիբեռզենքերով իրականացված ցանկացած հարձակում պետք է համապատասխանի ՄՀԻ հիմնարար սկզբունքներին, իսկ միջազգային իրավունքի առկա կարգավորումները՝ համապատասխան ճկուն մեկնաբանության պարագայում բավարար են զինված հակամարտությունների ժամանակ կիբեռմիջոցների կիրառումը կարգավորելու համար: Եվ հաշվի առնելով կիբեռզենքերի իրավաչափությունը, հասանելիությունը, տեխնիկական առանձնահատկություններն ու արդյունավետությունը, կիբեռմիջոցների կիրառման մասով ՄՀԻ կանոնների մեկնաբանության առանձնահատկությունները, վերջին տասնամյակներում կիբեռմիջոցների կիրառման պրակտիկան ու ժամանակակից մարտահրավերները՝ տրամաբանական է, որ պետությունները ձեռնարկում են և պետք է ձեռնարկեն բոլոր անհրաժեշտ քայլերը կիբեռպաշտպանության ոլորտն ուսումնասիրելու, պետական տեսլականը ձևավորելու, սեփական ներուժն այս ոլորտում գնահատելու և զարգացնելու ուղղությամբ:

Կիբեռանվտանգությունը և կիբեռպաշտպանությունը որպես պետական պաշտպանության և միջազգային անվտանգության առանցքային բաղադրիչ

2010 թվականի ՆԱՏՕ-ի Լիսաբոնի գագաթնաժողովի ընթացքում պետությունների և կառավարությունների ղեկավարները քննարկել են կիբեռանվտանգության ապահովման հարցը որպես միջազգային անվտանգության առանցքային նոր մարտահրավերներից մեկը, շեշտելով, որ «կիբեռհարձակումները կարող են հասնել այնպիսի շեմի, որը սպառնում է ազգային և եվրատլանտյան անվտանգությանն ու կայունությանը»:[38] Կիբեռտարածությունը ստեղծել է

[37] Michael N. Schmitt (Editor-in-Chief) et. al., *Blue Book*, supra n. 31, 263.
[38] UN, Developments in the Field of Information and Telecommunications in the Context of International Security (Study Series 33) 27.

բացարձակ նոր անվտանգային միջավայր և ռիսկեր: 2016 թվականին ստորագրվեց կիբեռպաշտպանության վերաբերյալ ՆԱՏՕ-ի հանձնառությունը, որի առաջին կետով պետությունների և կառավարությունների ղեկավարները հանձն առան ապահովել, որ դաշինքը հետևի կիբեռվտանգների ոլորտում արագ տեղի ունեցող փոփոխություններին, և որ պետությունները պատրաստ կլինեն կիբեռտարածքում պաշտպանության կազմակերպմանն այնպես, ինչպես օդում, ցամաքում և ծովում: Նույն հանձնառությամբ նաև արձանագրվեց ՆԱՏՕ-ի և ԵՄ-ի միջև շարունակական համագործակցությունը կիբեռպաշտպանության ոլորտում[39]:[40] Արդեն 2016 թվականին ԱՄՆ պաշտպանության նախարար Էշթոն Քարթերը բացահայտ պաշտոնապես հայտարարել է այն մասին, որ ԴԱԻՇ-ի հետ պայքարում ավանդական զենքերի հետ մեկտեղ ԱՄՆ-ը կիրառում է նաև պատերազմ վարելու կիբեռմիջոցներ:[41] Իսկ Միացյալ Թագավորության պաշտոնյաները 2020 թվականին բացահայտել են Միացյալ Թագավորության պաշտպանության համակարգում սովորական ռազմական ուժերի կառուցվածքում ազգային կիբեռուժերի գործունեության մասին:[42] 2018 թվականի հունիսի 13-ին ԵՄ խորհրդարանն ընդունեց կիբեռպաշտպանության վերաբերյալ 2018/2004(INI) բանաձևը, որով, մասնավորապես, կիբեռպաշտպանության ոլորտում քաղաքականությունը և կարողությունները արձանագրվում են որպես Եվրոպական պաշտպանության միության զարգացման կարևորագույն տարր՝ անդրադառնալով նաև կիբեռդիմադրության, կիբեռզսպման և կիբեռպաշտպանության ոլորտում հետագա ռազմավարության ու կիբեռտարածքի կարգավորման իրավական նորմերին:[43] 2021

[39] 2016 թվականին ստորագրվել է նաև ԵՄ-ի և ՆԱՏՕ-ի առաջին համատեղ հռչակագիրը, որով ամրագրվեցին տարածաշրջանային պաշտպանության ոլորտում համագործակցության զարգացման հիմնական յոթ ուղղությունները, որոնց թվում է նաև կիբեռանվտանգությունն ու կիբեռպաշտպանությունը (Josep Borrell, High Representative of the EU for Foreign Affairs and Security Policy/Vice-President, https://www.eeas.europa.eu/sites/default/files/eu_nato_factshee_november-2020-v2.pdf, https://www.eeas.europa.eu/eeas/eu-nato-cooperation-factsheets_en):

[40] Cyber Defence Pledge, 08 July 2016, at: https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

[41] Ashton Carter, Interview by Rachel Martin "In Fight Against ISIS, U.S. Adds Cyber Tools", NPR (28 Feb 2016) audio, at: http://www.npr.org/templates/transcript/transcript.php?storyId=468446138.

[42] Gordon Corera, UK's National Cyber Force comes out of the shadows (20 Nov 2020) BBC news, at: https://www.bbc.com/news/technology-55007946.

[43] ԵՄ խորհրդարանի կիբեռպաշտպանության վերաբերյալ 2018 թվականի հունիսի 13-ի 2018/2004(INI) բանաձև (https://www.europarl.europa.eu/doceo/document/TA-8-2018-0258_EN.html)

թվականի հոկտեմբերի 7-ին ԵՄ խորհրդարանն ընդունեց կիբեռպաշտպանության կարողությունների վերաբերյալ 2020/2256(INI) բանաձևը:[44]

Պատահական չէ, որ վերջին տասնամյակների ընթացքում պետությունները արտաքին թշնամուց պետական պաշտպանության համատեքստում մեծ ուշադրություն են դարձնում նաև կիբեռպաշտպանությանը՝ առաջին հերթին մշակելով կիբեռպաշտպանության մասով պետության ռազմավարությունը:

Կիբեռտարածքի ռազմական օգտագործման ռազմավարական կարգավորման հիմնական միտումները

Կիբեռտարածքի ռազմական օգտագործման ռազմավարական մակարդակով կարգավորումը տեղի է ունենում երկու հիմնական ուղղություններով՝ 1) մշակելով և գործարկելով կիբեռպաշտպանության առանձին ռազմավարություն (կիբեռանվտանգության ռազմավարությանը զուգահեռ)՝ նպատակ ունենալով հստակ առանձնացնելու կիբեռտարածությունում պետության պաշտպանական գործողությունների իրականացման ձևերն ու մոտեցումները,[45] 2) կիբեռտարածքի ռազմական օգտագործման խնդիրները ներառելով կիբեռանվտանգության ռազմավարության մեջ, սակայն չնույնացնելով կիբեռանվտանգությունն ու կեբեռպաշտպանությունը և արտացոլելով կիբեռտարածությունում զինված ուժերի պաշտպանական գործողությունների առանձնահատկությունները, կամ էլ կարգավորելով կիբեռպաշտպանությունն ավելի լայն՝ պետական պաշտպանության ռազմավարության կամ զարգացման ծրագրի մեջ:[46] Երկու մոտեցումն էլ, մեր կարծիքով, առերևույթ ունեն իրենց առավելություններն ու թույլ կողմերը: Այսպես, կիբեռպաշտպանության հստակ տարանջատումը այլ ռազմական հարթակներից և կիբեռանվտանգությունից հնարավորություն է տալիս պետությանը ավելի նեղ մասնագիտացված մոտեցում ցուցաբերել, մանրամասն անդրադարձ կատարել կիբեռպաշտպանության իրավիճակի, տվյալ ոլորտում ռիսկերի և հատուկ կարիքների գնահատմանը և ծրագրել կիբեռպաշտպանության ու կիբեռպաշտպանությունն ապահովող ռազմական ուժերի հետագա զարգացման

[44] ԵՄ խորհրդարանի կիբեռպաշտպանության կարողությունների վերաբերյալ 2021 թվականի հոկտեմբերի 7-ի 2020/2256(INI) բանաձև (https://www.europarl.europa.eu/doceo/document/TA-9-2021-0412_EN.html):

[45] Օրինակ, Բելգիա, Չեխիա, Դանիա, Նիդեռլանդներ, Պորտուգալիա, ԱՄՆ և այլն (https://ccdcoe.org/library/strategy-and-governance/):

[46] Օրինակ, Էստոնիա, Իսլանդիա, Լիտվա, Չեռնոգորիա և այլն (https://ccdcoe.org/library/strategy-and-governance/):

ուղեծիրը: Սակայն, նման մոտեցման հնարավոր բացասական հետևանքը կայանում է նրանում, որ առանձին կիբեռպաշտպանության ռազմավարության շրջանակում հնարավոր է հաշվի չառնվի կիբեռտարածքում ռազմական և քաղաքացիական ենթակառուցվածքների փոխկապակցվածությունը, կիբեռպաշտպանության և ծովային, ցամաքային ու օդային պաշտպանության փոխկապակցվածությունը, ինչպես նաև կիբեռպաշտպանության և կիբեռանվտանգության հարաբերակցությունն ու փոխկապակցվածությունը: Միևնույն ժամանակ, պետության կիբեռպաշտպանության ոլորտը կիբեռանվտանգության ռազմավարության շրջանակում կամ պետության ավելի լայն ռազմական դոկտրինի շրջանակում կարգավորելը կարող է հանգեցնել կիբեռպաշտպանությանը ոչ բավարար ուշադրությանը ռազմավարական տեսանկյունից և որպես հետևանք՝ ավելի խոցելի կիբեռպաշտպանությանը: Այստեղ նաև հարկ է ընդգծել, որ «կիբեռանվտանգություն» և «կիբեռպաշտպանություն» հասկացությունների իրավական հստակ բովանդակությունը և վերոհիշյալ հասկացությունների տարբերության վերաբերյալ միասնական պատկերացումը բացակայում են:[47] Որոշ մասնագետների կարծիքով, պայմանավորված կիբեռտարածքի առանձնահատկություններով կիբեռանվտանգության և կիբեռպաշտպանության տարբերության խնդիրն արհեստական է, և դրանք չեն կարող հստակ տարանջատվել պրակտիկայում:[48] Առկա է նաև կարծիք, որ կիբեռանվտանգությունը ենթադրում է վտանգներից և ռիսկերից պաշտպանությունն ու պաշտպանության որակը, իսկ կիբեռպաշտպանությունը՝ ռազմական հարձակմանը դիմակայելու և դրան հակահարված հասցնելու կարողությունն ու վերոհիշյալ նպատակներին ուղղված գործողությունները: Մասնագետների մի մասն էլ տարբերակում է պասիվ կիբեռպաշտպանություն, որը ներառում է նաև անվտանգային տարրեր և կիրարկվում է սուբյեկտի ներքին կիբեռենթակառուցվածքներում, և ակտիվ կիբեռպաշտպանությունը, որի հիմնական իմաստը սուբյեկտի ներքին կիբեռենթակառուցվածքների և «հակառակորդի» ենթակառուցվածքներում հակազդման նպատակով հարձակողական բնույթի կիբեռմիջոցառումների իրականացման մեջ է:[49] Առերևույթ, կիբեռանվտանգություն և կիբեռպաշտպանություն հասկացությունների միջև տարբերության այսպիսի

[47] Damjan Štrucl, Comparative study on the cyber defence of NATO Member States, p. 21.
[48] Damjan Štrucl, *ibid.*, p. 21 citing Da Silva, M., F., 2016, Cyber Security vs. Cyber Defense: A Portuguese view in the distinction. Cyberlaw: CIJIC, p. 1-2 (https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf).
[49] Damjan Štrucl, supra n. 47, p. 21.

վերացական բնույթով ու անորոշությամբ է պայմանավորվում տարբեր պետությունների կողմից կիբեռպաշտպանության խնդիրները կիբեռանվտանգության համատեքստում կամ ավելի լայն՝ ռազմական դոկտրինի համատեքստում կարգավորելը:

ԿԻԲԵՌՊԱՇՏՊԱՆՈՒԹՅԱՆ ՌԱԶՄԱՎԱՐԱԿԱՆ ԵՎ ԻՆՍՏԻՏՈՒՑԻՈՆԱԼ ԿԱՐԳԱՎՈՐՄԱՆ ՄԻՋԱԶԳԱՅԻՆ ՓՈՐՁԸ

ՉԵԽԻԱ

Ռազմավարական իրավական կարգավորումները

Չեխիայում ազգային անվտանգության և պետական պաշտպանության ոլորտում ռազմավարական նշանակության փաստաթղթերը, որոնցում անդրադարձ է կատարվում կիբեռպաշտպանությանը, երկրի անվտանգության ռազմավարությունն է, պետական պաշտպանության վերաբերյալ սպիտակ թուղթը, պետական պաշտպանության 2030թ. երկարաժամկետ հեռանկարների վերաբերյալ փաստաթուղթը, Չեխիայի Հանրապետության զինված ուժերի կազմավորման հայեցակարգը, Չեխիայի պետական պաշտպանության ռազմավարությունը:[50] 2018 թվականին Չեխիայում ընդունվել է նաև առանձին կիբեռպաշտպանության ռազմավարություն (2018-2022):[51] Հատկանշական է, որ Չեխիայի կիբեռպաշտպանության ռազմավարության շրջանակում կիբեռպաշտպանությունը որակվում է որպես կիբեռանվտանգության հասկացության հատուկ և ինքնավար ճյուղ, դիտարկվում է որպես պետական պաշտպանության բաղկացուցիչ տարր և ապահովվում է «Չեխիայի Հանրապետությունում պաշտպանության ապահովման մասին» օրենքով:[52] Միևնույն ժամանակ, նշվում է, որ կիբեռպաշտպանության հիմնական տարբերությունը կիբեռանվտանգությունից կայանում է կիբեռտարածքում «հարձակումների» բնույթի և ինտենսիվության մեջ, և կիբեռպաշտպանությունը սկսում է կիրարկվել միայն «ամենաինտենսիվ հարձակումների» ժամանակ, մինչդեռ «կիբեռանտվանգություն» և «կիբեռպաշտպանություն» հասկացությունների տարբերակման հստակ

[50] Tomáš Minárik Revised and updated by Tat'ána Jančárková, National Cyber Security Organisation: CZECHIA, p. 15 (https://ccdcoe.org/uploads/2018/10/CS_organisation_CZE-3.0_Revised_TJ_Final_PDF.pdf).
[51] Cyber Defense Strategy of the Czech Republic 2018-2022, National Cyber Operations Center, at: https://www.vzcr.cz/uploads/69-Cyber-Defence-Strategy-2018.pdf
[52] *Ibid.*, p. 1.

չափանիշները բացակայում են:[53] Ռազմավարության ներածական հատվածում նաև նշվում է, որ Չեխիայի կիբեռպաշտպանության ռազմավարությունը բաղկացած է երկու հատվածից՝ հրապարակային, որն ավելի ընդհանրական բնույթ ունի և ձևակերպում է պետության տեսլականը, նպատակներն ու խնդիրներն այս ուղղությամբ, և ոչ հրապարակային, որտեղ նկարագրվում են բոլոր այն միջոցառումները, որոնք պետք է իրականացվեն համապատասխան խնդիրների լուծման համար:[54] Կառուցվածքային առումով Չեխիայի կիբեռպաշտպանության ռազմավարության հրապարակային հատվածում վերլուծված են կիբեռպաշտպանության ոլորտում Չեխիայի առջև ծառացած հիմնական մարտահրավերները, ներկայացված է պետության տեսլականն ու ռազմավարական վեկտորը, որի համաձայն Չեխիայի կիբեռպաշտպանության ռազմավարության հիմնական նպատակն է հասնել մի իրավիճակի, երբ տվյալ ոլորտում իրավասու պետական մարմինը կարողանա երաշխավորել Չեխիայի Հանրապետության կիբեռպաշտպանությունը, կիբեռտարածքում իրականացնել ռազմական օպերացիաներ և միջազգայնորեն ունենալ ակտիվ դերակատարում : Որպես վերոհիշյալ նպատակին հասնելու եղանակ՝ սահմանվում են իրավական դաշտը, կիբեռպաշտպանության ոլորտում իրավասու մարմնի ենթակառուցվածքների ձևավորմանն ու զարգացմանը, կիբեռտարածքում պաշտպանական կարողությունների զարգացումը, կրթական ոլորտում համագործակցության ձևավորումը և կրթական ծրագրերի իրականացումը, պաշտպանության նախարարության մասնակցությունը կիբեռանվտանգության ապահովման հարցում: Եվ վերջապես, ռազմավարության վերջին հատվածը նվիրված է ռազմավարական նպատակի և խնդիրների իրականացմանը և եզրահանգումներին:[55]

Ինստիտուցիոնալ կարգավորումները

Ինստիտուցիոնալ առումով ռազմական կիբեռպաշտպանությունն իրականացվում է զինված ուժերի ենթակայությամբ գործող Հաղորդակցության և տեղեկատվական համակարգերի գործակալությունը, որն ունի մի շարք գործառույթներ զինված ուժերի և պաշտպանության նախարարության համակարգերում:[56] Մինչդեռ պաշտպանության նախարարության և ազգային

[53] *Ibid.*, p. 2.
[54] *Ibid.*
[55] *Ibid.*, pp. 6-16.
[56] Tomáš Minárik, supra n. 50, p. 16.

անվտանգության ծառայության միջև առկա համագործակցության հուշագրով կարգավորվում է, inter alia (ի թիվս այլոց), կիբեռտարածքի անվտանգության հետ կապված նշված մարմինների համագործակցության շրջանակը: Եվ վերջապես, ռազմական հետախուզության համակարգում առանձին ինստիտուցիոնալ կառույց պետք է զբաղվի կիբեռտարածքում ռազմական հետախուզության հետ կապված խնդիրներով:[57]

ԷՍՏՈՆԻԱ

Ռազմավարական իրավական կարգավորումները

Էստոնիայում կիբեռպաշտպանության ռազմավարական հիմքերն արտացոլված են Էստոնիայի ազգային անվտանգության հայեցակարգում, ինչպես նաև պետական պաշտպանության զարգացման 2017-2026թթ. ծրագրում: Մասնավորապես, Էստոնիայի ազգային անվտանգության հայեցակարգում կիբեռպաշտպանության կազմակերպումը դիտվում է որպես հայեցակարգի հիմնական նպատակին հասնելու համար անհրաժեշտ միջոցառումներից մեկը:[58] Նույն փաստաթղթի համաձայն կիբեռանվտանգությունը կազմակերպելու համար Էստոնիան կիրառում է միասնական լուծումներ խաղաղության ժամանակ և զինված հակամարտությունների ժամանակ, միևնույն ժամանակ դիտարկելով կիբեռպաշտպանությունը որպես պետական պաշտպանության համակարգի մաս:[59] Մինչդեռ պետական պաշտպանության զարգացման 2017-2026թթ. ծրագրով կրկին վերահաստատվում է, որ կիբեռտարածքն առանձին ռազմական հարթակ է, որտեղ պետական պաշտպանությունն ապահովելու համար որոշում է կայացվել ստեղծել Էստոնիայի զինված ուժերի կիբեռհրամանատարություն: Կիբեռհրամանատարության հիմնական առաքելությունն է պաշտպանել Էստոնիայի և նրա դաշնակիցների տեղեկատվական համակարգերը հակառակորդների գործողություններից և ըստ անհրաժեշտության իրականացնել կիբեռօպերացիաներ ընդդեմ հակառակորդի:[60]

---

[57] Tomáš Minárik, supra n. 50, p. 16-17.
[58] National Security Concept of Estonia 2017, at: https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf, p. 7.
[59] *Ibid.*, p. 16.
[60] National defense development Plan of Republic of Estonia 2017-2026, at: https://www.kaitseministeerium.ee/riigikaitse2026/arengukava/eng/

Ինստիտուցիոնալ կարգավորումները

Ինստիտուցիոնալ առումով կիբեռպաշտպանության համակարգումը իրականացնում է Էստոնիայի պաշտպանության նախարարությունը, որի համակարգում 2014 թվականից սկսած՝ մի առանձնացված ստորաբաժանում պատասխանատու է, մասնավորապես, պետության կիբեռպաշտպանության քաղաքականության համար: Էստոնիայի պաշտպանության նախարարությունը սերտորեն համագործակցում է ՆԱՏՕ-ի հետ՝ կիբեռպաշտպանության ոլորտում վարժանքներ և գործնական ու կրթական միջոցառումներ անցկացնելու նպատակով:[61] Բացի պաշտպանության նախարարությունից, Էստոնիայում կիբեռպաշտպանության կազմակերպմանն աջակցում է նաև Պաշտպանության լիգայի՝ կամավոր, կազմակերպված համակարգ ունեցող և զինված պաշտպանական կազմակերպության, կիբեռպաշտպանության բաժինը, որը համալրված է հանրային և մասնավոր կազմակերպություններից կիբեռանվտանգության մասնագետներով:[62] Ճգնաժամային իրավիճակների կանխարգելումն ու ճգնաժամի կառավարումը բոլոր ուղղություններով, այդ թվում՝ կիբեռտարածքում և ներառյալ՝ կրիտիկական ենթակառուցվածքների պաշտպանությունը, համակարգում է Էստոնիայի ներքին գործերի նախարարությունը՝ համագործակցելով տնտեսական հարցերի և կապի նախարարության հետ:[63] Այսպիսով, թերևս Էստոնիայի հանրորեն հասանելի փաստաթղթերը չեն տալիս երկրի կիբեռպաշտպանության ռազմավարության ավելի մանրամասն պատկերը, բայց կարելի է եզրահանգել, որ Էստոնիան առանձնահատուկ ուշադրություն է դարձնում հենց կիբեռպաշտպանությանը՝ պաշտպանության նախարարության և զինված ուժերի համատեքստում՝ ընդհուպ մինչև ստեղծելով առանձին կառուցվածքային միավոր հենց կիբեռմիջոցներով ռազմական գործողություններին դիմակայելու և պատասխան ռազմական գործողություններ իրականացնելու նպատակով:

---

[61] Anna-Maria Osula Researcher (Kadri Kaska ed.), National Cyber Security Organisation: Estonia, Tallinn 2015, p. 9-10, at: https://ccdcoe.org/uploads/2018/10/CS_organisation_ESTONIA_032015_1-1.pdf (citing Estonian Ministry of Defence, Estonian National Defence Strategy, 2011; Estonian Ministry of Defence, 'Ministry of Defence to Establish Cyber Policy Department', 2013; Estonian Ministry of Defence, 'NATO Secretary General Thanks Estonia for Offer of Cyber Range', 2014; Eesti Kaitsevägi, 'Terras: NATO kavandab eestisse küberharjutusvälja loomist', 2014).

[62] *Ibid.,* p. 10 (citing Kaitseliit, 'Estonian Defence League's Cyber Unit').

[63] *Ibid.,* p.11 (citing Emergency Act §§ 34, 36, Sorainen, Kriisireguleerimise valdkonna juriidiline analüüs, 2013).

ԼՅՈՒՔՍԵՄԲՈՒՐԳ

Ռազմավարական իրավական կարգավորումները

Կիբեռպաշտպանության ոլորտը Լյուքսեմբուրգում արտացոլված է Ազգային կիբեռանվտանգության ռազմավարությունում, որտեղ որպես թվային ենթակառուցվածքների պաշտպանության ապահովմանը հասնելու համար յոթ խնդիրների թվում է նաև կիբեռպաշտպանության ապահովումը: Նշված կետով արձանագրված է, մասնավորապես, որ 2017 թվականի հուլիսին Լյուքսեմբուրգի կառավարությունը հաստատել է 2025 թվականի համար և դրանից հետո կիբեռթիրախներ ընտրելու ուղեցույցը, պահպանվել է կիբեռպաշտպանության ոլորտում հմտությունների ու կարողությունների շարունակական զարգացումն ապահովելու հանձնառությունը, իսկ Լյուքսեմբուրգի պաշտպանությունը (արտաքին գործերի նախարարության պաշտպանության վարչությունն ու Լյուքսեմբուրգի զինված ուժերը) հանձն է առել շարունակել կիբեռանվտանգության ազգային և միջազգային ռազմավարությունների իր պատասխանատվության ներքո գտնվող տարրերի սահմանման և կիրարկման աշխատանքը:[64] Այսպիսի ձևակերպումից կարելի է եզրահանգել, որ Լյուքսեմբուրգը դիտարկում է կիբեռպաշտպանությունը որպես կիբեռանվտանգության առանձին տարր: Պետության կիբեռպաշտպանության վերաբերյալ դրույթներ տեղ են գտել նաև 2025 թվականի և դրանից հետոյի համար Լյուքսեմբուրգի պաշտպանական ուղեցույցներում:[65] Այս ուղեցույցով որպես նոր մարտահրավեր նշվում է կիբեռհարձակումների և կիբեռտարրեր պարունակող հիբրիդային հարձակումների պարագայում պաշտպանությունը, դիտարկելով կիբեռտարածքը որպես զինված հակամարտություններ վարելու հարթակ՝ դասական հարթակների հետ զուգահեռ,[66] իսկ Լյուքսեմբուրգը այս ուղղությամբ նախատեսել է ձեռնարկել միջոցառումներ, մասնավորապես, կիբեռկարողությունների զարգացման համար՝ ապահովելու, որ բոլոր մարմիններն ու հանրային ծառայությունները բնականոն աշխատեն, իսկ

[64] Luxembourg, National Cyber Security Strategy III (2018-2020), p. 21, at: https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf.

[65] Luxembourg Defence Guidelines for 2025 and Beyond, Ministry of Foreign and European Affairs Defence Directorate, 2017, https://defense.gouvernement.lu/dam-assets/la-defense/luxembourg-defence-guidelines-for-2025-and-beyond.pdf.

[66] *Ibid.*, pp. 12, 37, 43, 44 https://defense.gouvernement.lu/dam-assets/la-defense/luxembourg-defence-guidelines-for-2025-and-beyond.pdf.

քաղաքացիական անձինք և ենթակառուցվածքները լինեն պաշտպանված:[67] Միևնույն ժամանակ, գիտակցելով կիբեռպաշտպանության կազմակերպման առանձնահատկությունները, Լյուքսեմբուրգում մշակվել է նաև առանձին Կիբեռպաշտպանության ռազմավարություն:[68] Կիբեռպաշտպանության ռազմավարությամբ ամրագրվում է Լյուքսեմբուրգի երկարաժամկետ նպատակը, այն է՝ մինչև 2030 թվականը ստեղծել ՆԱՏՕ և ԵՄ երկրների ամենաապահով կիբեռպաշտպանության համակարգերից՝ առավելագույնին հասցնելով իր կիբեռպաշտպանության կարողությունները:[69] Նշված նպատակին հասնելու համար Ռազմավարությունում նկարագրված են այն խնդիրները, որոնք ենթակա են լուծման, մասնավորապես՝ արհեստավարժ և մոտիվացված անձնակազմ ունենալը, կիբեռպաշտպանության ոլորտում ամուր ազգային և միջազգային համագործակցությունը, կիբեռպաշտպանության ինտեգրումը պաշտպանության ոլորտում բոլոր գործողություններում, ակտիվներում և մշակույթում, կիբեռպաշտպանության ապագա զարգացումների քարտեզագրումը, նախապատվությունների սահմանումն ու գիտահետազոտական ծրագրերի իրականացումը:[70] Ռազմավարությամբ նախատեսվում է նաև հիմնական նպատակի և խնդիրների իրականացման նկատմամբ մշտադիտարկման և արդյունքների գնահատման ծրագիր:[71]

Ինստիտուցիոնալ կարգավորումները

Ինստիտուցիոնալ առումով կիբեռպաշտպանության ոլորտում հիմնական գործառույթները Լյուքսեմբուրգի պաշտպանության իրավասության ներքո են, իսկ կիբեռպաշտպանության ոլորտում արտակարգ իրավիճակների կառավարման հիմնական գործառույթները՝ համակարգչային արտակարգ իրավիճակների արձագանքման թիմի, միաժամանակ, կիբեռպաշտպանության ապահովումը տեղի է

[67] *Ibid.*, pp. 20, 29, https://defense.gouvernement.lu/dam-assets/la-defense/luxembourg-defence-guidelines-for-2025-and-beyond.pdf
[68] Luxembourg Cyber Defense Strategy (2021-2031), The Government of the Grand Douchy of Luxembourg, Ministry of Foreign an European Affairs – Directorate of Defence (Feb 2021), https://ccdcoe.org/uploads/2018/10/Luxembourg_Cyber-Defence-Strategy_2021_English.pdf.
[69] *Ibid.*, p. 9.
[70] *Ibid.*, p. 11-15.
[71] Ibid., p.17.

ունենում տարբեր կառույցների միջև արդյունավետ համագործակցության արդյունքում:[72]

ԹՈՒՐՔԻԱ

Ռազմավարական իրավական կարգավորումները

Թուրքիայում 2016-2019թթ. գործում էր Ազգային կիբեռանվտանգության ռազմավարությունը: Հրապարակային առկա տեղեկատվության համաձայն 2020 թվականին Թուրքիայում ընդունվել է կիբեռանվտանգության գործողությունների նոր ծրագիր 2020-2023 թվականների համար՝ մշակված Թուրքիայի տրանսպորտի և ենթակառուցվածքների նախարարության կողմից՝ համագործակցելով ՀԿ-ների, համալսարանների, հանրային և մասնավոր սեկտորների հետ: Թուրքիայի կիբեռանվտանգության ռազմավարությունն ու գործողությունների ծրագիրը ներառում է 40 գործողություն և ռազմավարական նպատակների իրականացմանն ուղղված 75 միջոցառում:

Ինստիտուցիոնալ կարգավորումները

Ինստիտուցիոնալ տեսանկյունից կիբեռտարածքում պաշտպանվածության մակարդակը բարձրացնելու նպատակով Թուրքիայում տեղեկատվական տեխնոլոգիաների և կապի իրավասու մարմնի համակարգում հիմնադրվել է Ազգային կիբեռանվտանգության միջամտության կենտրոնը: Թեև Թուրքիայի կիբեռանվտանգության ռազմավարության և գործողությունների ծրագրի տեքստը հրապարակված չէ, սակայն հրապարակված հաղորդագրության վերլուծությունը թույլ է տալիս եզրահանգել, որ կիբեռանվտանգության ռազմավարության համատեքստում անդրադարձ է կատարված նաև պետության կիբեռպաշտպանությանը:[73] 2020 թվականի համաշխարհային կիբեռանվտանգության ինդեքսի հրապարակած տվյալների համաձայն՝ Թուրքիայի գնահատականը՝ 97,49 և Թուրքիան տասնմեկերորդն է կիբեռանվտանգության հուսալիության տեսանկյունից:[74] Իսկ ազգային կիբեռանվտանգության ինդեքսով

[72] Philippe Mitsuya Zotz, National Cybersecurity Organisation: Luxembourg, Tallinn 2021, p. 19.
[73] Turkey reveals its three-year cyber security plan, 30 Dec 2020, at: https://www.trtworld.com/magazine/turkey-reveals-its-three-year-cybersecurity-plan-42820.
[74] Global Cybersecurity Index 2020 (published in Geneva 2022), at: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

2020 թվականի դրությամբ Թուրքիան հիսունյոթերորդն է՝ ունենալով բարձր ցուցանիշ քաղաքականության մշակման առումով (86%), բավարար ցածր ցուցանիշ կիբեռտարածքում վտանգների վերլուծության տեսանկյունից (20%), բավարար բարձր ցուցանիշ կրթության և մասնագիտական զարգացման տեսանկյունից (44%), բավարար բարձր ցուցանիշ կիբեռտարածքում ճգնաժամի կառավարման տեսանկյունից (60%) և նվազագույն բավարար ցուցանիշ ռազմական ոլորտում կիբեռօպերացիաների կազմակերպման կարողությունների տեսանկյունից (17%):[75]

ԻՍՐԱՅԵԼ

Ռազմավարական իրավական և ինստիտուցիոնալ կարգավորումները

Հետաքրքիր է Իսրայելի փորձը՝ կիբեռպաշտպանության կազմակերպման օրինակը, որպես կիբեռանվտանգության և կիբեռպաշտպանության ոլորտում աշխարհի առաջատարներից մեկը: Այսպես, Իսրայելը որդեգրեց կիբեռտարածքի և թվային տեխնոլոգիաների զարգացման ուղղությունը դեռևս 1990-ականների վերջին: Իսկ կիբեռպաշտպանության ուղղությամբ առաջին ռազմավարական քայլերն Իսրայելի կողմից պաշտոնապես ձեռնարկվել են Իսրայելի կառավարության 2011 թվականի թիվ 3611 բանաձևով:[76] Այս բանաձևով նախատեսվում էր ստեղծել Ազգային կիբեռբյուրո և ամրապնդել բնականոն կյանքի ապահովման համար էական նշանակության ունեցող ենթակառուցվածքների պաշտպանությունը կիբեռհարձակումներից:[77] Իսրայելի պաշտպանական ուժերի 2015 թվականի ռազմավարությամբ որոշվեցին կիբեռպաշտպանության կատարելագործման ուղղությունները, ներառյալ՝ կիբեռտարածքի պաշտպանության ամրապնդումը՝ այն հասցնելով Իսրայելի հետախուզական, օդային և ռազմածովային գերակայության հետ հավասար մակարդակի, Իսրայելի կիբեռպաշտպանական և կիբեռհարձակողական գործողությունների մասով պատրաստվածության ամրապնդումը, Իսրայելի պաշտպանական ուժերի կառուցվածքում կիբեռպաշտպանության ստորաբաժանման ձևավորումը, Իսրայելի զինված ուժերի

[75] National Cyber Security Index (NCSI) for Turkey, at: https://ncsi.ega.ee/country/tr/.
[76] Իսրայելում կիբեռպաշտպանության ռազմավարության ժամանակագրական զարգացումը ավելի մանրամասն ներկայացված է՝ Jasper Frei, Israel's National Cybersecurity and Cyberdefense Posture Policy and Organizations, Zürich, September 2020, Cyber Defense Project (CDP) Center for Security Studies (CSS), ETH Zürich, p.6, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf.
[77] Cyber Security Portal, United Nations Institute for Disarmament Research (UNIDIR), Israel page last reviewed in August 2022, at: https://cyberpolicyportal.org/states/israel.

կիբեռկարողությունների զարգացումն՝ ապահովելու երկրի զինված ուժերի բնականոն գործունեությունը նույնիսկ հարձակումների ընթացքում, կիբեռպատերազմի կարողությունների զարգացումը Իսրայելի ռազմավարական և մարտավարական զսպման կարողություններն ուժեղացնելու նպատակով:[78] 2017 թվականին ընդունվեց Իսրայելի կիբեռանվտանգության ռազմավարությունը, որի երկու կարևորագույն ուղղություններն են ակտիվ կիբեռպաշտպանությունն ու կիբեռպաշտպանական օպերացիաները: Տվյալ ոլորտում Իսրայելի պաշտպանական ուժերի կողմից որդեգրած մոտեցումը հիմնված է Դավիդ Բեն Գուրիոնի դոկտրինալ սկզբունքների վրա, դրանք են՝ հնարավոր հարձակումների զսպումը, պետության, Իսրայելի բնակչության, ենթակառուցվածքների և շահերի պաշտպանությունը, տեխնոլոգիական գերազանցության և որակի առավելության հասնելու վճռականությունը, հաղթանակը, վաղ նախազգուշացման կարողությունների զարգացումը, ազդեցիկ պետությունների հետ դաշինքների ձևավորումը:[79] Ընդ որում, կիբեռոլորտում ռազմավարությամբ կարողությունների զարգացումը պաշտոնապես ուղղված է Իսրայելի թշնամիներին դիմակայելու համար, որոնց թվում են նաև Սիրիան, Իրանը, Լիբանանը: 2017 թվականի կիբեռանվտանգության ռազմավարության գործողությունների ծրագիրը հանրայնացված չէ:[80] 2017 թվականին Իսրայելի կառավարության թիվ 3270 բանաձևով նաև ստեղծվում է Իսրայելի ազգային կիբեռգրասենյակը (ԻԱԿ)՝ միավորելով Իսրայելի ազգային կիբեռբյուրոն և Ազգային կիբեռանվտանության մարմինը:[81] ԻԱԿ-ը գործում է Իսրայելի վարչապետի անմիջական համակարգման ներքո և կազմում է վարչապետի գրասենյակի կառուցվածքային մասը:[82] ԻԱԿ-ը տարբեր ուղղություններով համագործակցում է Իսրայելի պաշտպանության նախարարության, հանրային անվտանգության նախարարության, և այլ նախարարությունների հետ:[83] Հարկ է նաև ընդգծել, որ Իսրայելն այն պետություններից է, որ 2000-ական թվականներից բացահայտ փորձարկում է կիբեռմիջոցների կիրառումը՝ պաշտպանական համատեքստում: Այսպես, օրինակ, 2007 թվականին Իսրայելն օգտագործելով կիբեռմիջոցներ՝ խոցելու համար Սիրայի հակաօդային պաշտպանությունը, իրականացրեց հարձակում Սիրիայում գտնվող օբյեկտի վրա, որտեղ ենթադրաբար իրականացվում էր միջուկային զենքի մշակում,

[78] *Ibid.*
[79] Jasper Frei, supra n. 76, p.9.
[80] *Ibid.*, p.11.
[81] Cyber Security Portal, UNIDIR, supra n. 77.
[82] Jasper Frei, supra n.76, pp.5 and 7.
[83] Jasper Frei, supra n.76, p. 14.

իսկ 2011 թվականին գործարկվեց ենթադրաբար Իսրայելի և ԱՄՆ-ի կողմից մշակված «Սթաքսնեթ» համակարգչային որդը՝ ընդդեմ Իրանի:[84]

ԱՅԼ

Հարկ է նաև հավելել, որ ուսումնասիրված մի շարք երկրներում, մասնավորապես, Բուլղարիայում,[85] Խորվաթիայում,[86] Դանիայում,[87] Ֆրանսիայում,[88] Գերմանիայում,[89] Հունգարիայում,[90] Իտալիայում,[91] Լատվիայում,[92] Լիտվայում,[93]

---

[84] *Ibid.*, p. 6.

[85] White paper on defence and the armed forces of the Republic of Bulgaria, decision № 239 of April 14th 2011 on adoption of the National Defense Strategy, Ministry of Defense of the Republic of Bulgaria, clauses 13, 113, 119, 120, at: https://ccdcoe.org/uploads/2018/10/Bulgaria_National-Defense-Strategy_2011_English-1.pdf; Cyber Resilient Bulgaria 2020 in Cyber Policy Portal, UNIDIR, page on Bulgaria last reviewed in June 2022, at: https://cyberpolicyportal.org/states/bulgaria.

[86] National security strategy the Republic of Croatia (2017), at: https://www.soa.hr/files/file/National-Security-Strategy-2017.pdf, e.g. pp. 11, 15-16; The Croatian Armed Forces Long–Term Development Plan 2015–2024, The Republic of Croatia Ministry of Defense, pp. 27-28, 77, at: https://www.morh.hr/wp-content/uploads/2018/01/ltdp_en_2015.pdf.

[87] Defence Agreement 2018 – 2023 (The Danish Government, the Liberal Alliance and the Conservatives) and the Social Democrats, the Danish People's Party and the Social-Liberal Party), at: https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-danish-defence-agreement-2018-2023-pdfa-2018.pdf; https://www.fmn.dk/en/topics/agreements-and-economi/agreement-for-danish-defence-2018---2023/.

[88] Strategic review of cyber defence, Secretary General for Defense and National Security, France, February 2018, at: http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf; France publishes a white paper on the Application of International Law in Cyberspace, 9 Sep 2019, at: https://dig.watch/updates/france-publishes-white-paper-application-international-law-cyberspace; Defence and National Security Strategic Review 2017, pp. 33-34, at: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/DEFENCE%20AND%20NATIONAL%20SECURITY%20STRATEGIC%20REVIEW%202017.pdf.

[89] Cyber Security Strategy for Germany 2021, Federal Ministry of the Interior, Building and Community, https://ccdcoe.org/uploads/2018/10/Germany_cyber-security-strategy-2021_English.pdf, clause 6. 4. 1. , 6. 4. 2. , 8. 3. 13, etc.

[90] Cyber Defense Concept of the Hungarian Defence Forces, Cyber Policy Portal, UNIDIR, page on Hungary last reviewed in June 2022, at: https://cyberpolicyportal.org/states/hungary; Hungarian Defence Force's Cyber Training Centre officially inaugurated, website of the Hungarian Government (Ministry of Defense), 14 June 2019, at: https://2015-2019.kormany.hu/en/ministry-of-defence/news/hungarian-defence-force-s-cyber-training-centre-officially-inaugurated.

[91] Luca Peruzzi, Italy's Multi-Year Planning document (Ministry of Defense) 2021-2023, at: https://euro-sd.com/2021/10/articles/exclusive/24116/italys-defence-multi-year-planning-document-2021-2023/; Cyber Policy Portal, UNIDIR, page on Italy last reviewed in September 2022, at: https://cyberpolicyportal.org/states/italy.

[92] National armed forces cyber defence unit (CDU) concept, Republic of Latvia Ministry of Defence, Riga 2013, at: https://www.mod.gov.lv/sites/mod/files/document/cyberzs_April_2013_EN_final.pdf;

Նիդեռլանդներում,[94] Հյուսիսային Մակեդոնիայում,[95] Նորվեգիայում,[96] Լեհաստանում[97] և բազմաթիվ այլ եվրոպական երկրներում, ինչպես նաև ԱՄՆ-ում[98] և Կանադայում[99] կիբեռտարածքը պետության կողմից որակվում է որպես հնարավոր ռազմական գործողությունների տարածք՝ օդային, ցամաքային և ջրային տարածքների հետ հավասարապես, փորձում են անդրադարձ կատարել կիբեռզենքերի առանձնահատկություններին՝ համեմատած զենքի սովորական տեսակների հետ, սահմանել որոշակի նպատակներ և խնդիրներ՝ կիբեռհարձակմանը դիմակայելու, կիբեռպաշտպանության և կիբեռզսպման համար գործողությունների ծրագրով:

Cybersecurity Strategy of Latvia 2019–2022 Informative Statement, Riga 2019, e.g. pp. 3, 6, 9, 13, 14, at: https://www.mod.gov.lv/sites/mod/files/document/Cybersecurity%20Strategy%20of%20Latvia%202019_2022.pdf.

[93] Vytautas Butrimas (Kadri Kaska ed.), National cyber security organization, Lithuania, Tallinn 2015, pp. 11-12, https://ccdcoe.org/uploads/2018/10/CS_organisation_LITHUANIA_092015-2.pdf.

[94] Dutch Ministry of Defense, Defense Cyber Strategy 2018: "Investing in digital military capability" (unofficial full translation), at: https://blog.cyberwar.nl/2018/11/dutch-defense-cyber-strategy-2018-investing-in-digital-military-capability-unofficial-translation/.

[95] Republic of Macedonia National cyber security strategy 2018 -2022, Version 1.2. (July 2018), pp. 24-26, at: https://ccdcoe.org/uploads/2021/02/North-Macedonia_National-Cyber-Security-Strategy-2018-2022_2018_English.pdf.

[96] National Cyber Security Strategy for Norway, Norwegian Ministries, clauses 1. 2. , 2. 2. , 3. 4, at: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf.

[97] Cybersecurity Doctrine of the Republic of Poland, National Security Bureau, 2015, at: https://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.html.

[98] Ի թիվս բազմաթիվ ռազմավարական փաստաթղթերի, հատուկ ուշադրության են արժանի ԱՄՆ Ներքին անվտանգության նախարարության 2018թ. մայիսի 5-ի կիբեռանվտանգության ռազմավարությունը, որով ծրագրվում է 2023 թվականին ունենալ լրամշակված և թարմացված ռազմավարություն (https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf) և Պաշտպանության նախարարության 2018թ. կիբեռռազմավարությունը, որի հանրայնացման ենթակա հակիրճ բովանդակությունը հասանելի է հետևյալ կայքում՝ https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF:

[99] Strong, Secured, and Engaged: Canada's Defense Policy (archived content), March 2020, at: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/defence-policy.html; National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure, Her Majesty the Queen in Right of Canada, as represented by the Minister of Public Safety and Emergency Preparedness, 2021, at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf.

ԿԻԲԵՌՊԱՇՏՊԱՆՈՒԹՅԱՆ ՌԱԶՄԱՎԱՐԱԿԱՆ ԵՎ ԻՆՍՏԻՏՈՒՑԻՈՆԱԼ ԿԱՐԳԱՎՈՐՄԱՆ ՄԻՋԱԶԳԱՅԻՆ ՓՈՐՁԻ ՎԵՐԼՈՒԾՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ԵԶՐԱՀԱՆԳՈՒՄՆԵՐԸ

Այսպիսով, հետապնդելով նույն ընդհանրական նպատակը՝ պետությունների սահմանած խնդիրները և ծրագրված գործողությունները կիբեռպաշտպանության տեսանկյունից հաճախ տարբերվում են. ավելին, որոշ դեպքերում հրապարակային հասանելի ռազմավարությամբ չեն սահմանվում բոլոր մանրամասները, որոնք հնարավոր է ռազմավարական տեսանկյունից դիտարկվեն որպես պետական գաղտնիք: Ինստիտուցիոնալ տեսանկյունից ազգային կիբեռպաշտպանության ծրագրերի մշակումը, համակարգումն ու իրականացումը, որպես կանոն, իրականացվում է պաշտպանության նախարարության և ՊՆ ենթակայությամբ գործող մարմինների կողմից՝ պաշտպանության համակարգում ստեղծելով հենց կիբեռպաշտպանության հարցերով զբաղվելու նպատակով ստեղծված առանձնացված ստորաբաժանում (ինչպես, օրինակ՝ ազգային կիբեռպաշտպանության կենտրոն կամ կիբեռպաշտպանության հրամանատարություն):[100] Որոշ երկրներում էլ կիբեռպաշտպանությունն իրականացվում է միջինստիտուցիոնալ համագործակցության միջոցով, մասնավորապես, ՊՆ և կապի ոլորտում համապատասխան նախարարության կողմից կամ ապակենտրոնացված եղանակով՝ յուրաքանչյուր պետական մարմնի կողմից՝ իր իրավասության ներքո գտնվող հարցերով:[101] Միևնույն ժամանակ, կարևոր եզրահանգում է, որ ուսումնասիրված գրեթե բոլոր պետություններում կիբեռպաշտպանության ոլորտում ռազմավարական փաստաթղթերը առկա են, դրանք սահմանված պարբերականությամբ վերանայվում և կատարելագործվում են՝ հաշվի առնելով նոր մարտահրավերները, այնպես, որ բացառվի այնպիսի ժամանակահատվածը, որի ընթացքում պետությունը չունենա կիբեռպաշտպանության ոլորտում պետական տեսլական, քաղաքականություն և ռազմավարական փաստաթղթեր:

[100] Damjan Štrucl, supra n.47, p. 50.
[101] Damjan Štrucl, *ibid.*

Կիբեռպաշտպանության ռազմավարական և ինստիտուցիոնալ կարգավորման առանձնահատկությունները ԱՊՀ տարածքի պետություններում [102]

ԲԵԼԱՌՈՒՍ

Բելառուսում ռազմավարական փաստաթղթերի մակարդակով կիբեռտարածքի պետական պաշտպանության նշանակությանը առերևույթ բավարար ուշադրության չի արժանացել: Բելառուսը 2015 թվականին ընդունել է Բելառուսի Հանրապետության թվայնացման զարգացման 2016-2022թթ. ռազմավարությունը,[103] որը, ինչպես կարելի է հասկանալ վերնագրից, առավելապես նվիրված է կառավարման տարբեր ոլորտներում, առավելապես մասնավոր-տնտեսական ուղղվածությամբ թվայնացման խթանմանը՝ առանց կիբեռտարածքի ռազմական օգտագործման բաղադրիչի: Ռազմավարությամբ հակիրճ անդրադարձ է կատարվում Բելառուսի ներքին գործերի մարմինների գործունեության շարունակական թվայնացման և սահմանային ծառայության տեղեկատվական համակարգի կատարելագործման անհրաժեշտությանը:[104] Բելառուսի ազգային անվտանգության 2010 թվականի հայեցակարգով «տեղեկատվական» անվտանգության ապահովումը դիտարկվում է որպես անձանց, հասարակությունն ու պետությունը արտաքին և ներքին «տեղեկատվական» վտանգներից պաշտպանելու պայման՝ սահմանելով տեղեկատվական անվտանգությունը որպես ազգային անվտանգության տարր՝ հստակ տարանջատելով այն ռազմական պաշտպանությունից:[105] Միևնույն ժամանակ, սկսած 2017 թվականից՝ Բելառուսն ու Ռուսաստանը քննարկում են միութենական պետության «տեղեկատվական անվտանգության» հայեցակարգը, որն առայժմ շարունակում է մնալ նախագիծ:[106]

---

[102] Սույն վերլուծությամբ Հայաստանի Հանրապետության փորձն ու ռազմավարական և ինստիտուցիոնալ կարգավորումների ներկա իրավիճակը ներկայացված է առանձին բաժնով:

[103] Постановление коллегии министерства связи и информатизации Республики Беларусь, 30 сентября 2015г. № 35, Стратегия развития информатизации в Распублике Беларусь на 2016-2022гг., по ссылке: http://nmo.basnet.by/informatization/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%8F%20%D1%80%D0%B0%D0%B7%D0%B2%D0%B8%D1%82%D0%B8%D1%8F%20%D0%B8%D0%BD%D1%84-%D0%B8%D0%B8%20%D0%BD%D0%B0%202016-2022%20%D0%B3%D0%B3.PDF.

[104] Ibid., c. 12.

[105] Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении концепции национальной безопасности Республики Беларусь», по ссылке: https://www.mil.by/ru/military_policy/basic/koncep/.

[106] Беларусь и Россия обсудили проект Концепции информационной безопасности Союзного государства, по ссылке: https://www.belta.by/politics/view/belarus-i-rossija-obsudili-proekt-kontseptsii-informatsionnoj-bezopasnosti-sojuznogo-gosudarstva-495901-2022/.

Թեև նախագծի հայեցակարգի տեքստը հրապարակայնացված չէ, սակայն առկա հրապարակային տեղեկատվությունից կարելի է եզրահանգել, որ դրանով անդրադարձ է կատարվելու նաև կիբեռտարածքի ռազմական օգտագործման մասով պետությունների քաղաքականությանն ու տեսլականին:[107] Եվ չնայած ռազմավարական փաստաթղթերի շրջանակում կիբեռտարածքի ռազմական պոտենցիալը կարծես անտեսված է, Բելառուսի պաշտպանության նախարարության համակարգում գործում է «ռադիոէլեկտրոնային պատերազմի զորքեր» անվանմամբ ստորաբաժանումը, որի հիմնական գործառույթներն են ռադիոէլեկտրոնային հետախուզությունը, ռադիոէլեկտրոնային հակաքայլերն ու ռադիոէլեկտրոնային պաշտպանությունը:[108] Ռադիոէլեկտրոնային պաշտպանության գաղափարը, սակայն, արմատապես տարբերվում է ժամանակակից կիբեռտարածքի ռազմական նշանակության գաղափարից:[109] Կիբեռտարածքում տեղի ունեցող միջադեպերին արձագանքման գործառույթը Բելառուսի նախագահի հովանու ներքո գործող համակարգչային միջադեպերին արձագանքման ազգային կենտրոնինն է, որը թերևս Բելառուսի ինստիտուցիոնալ համակարգում ամենամոտարկվածն է կիբեռպաշտպանության գործառույթին: Մինչդեռ, կիբեռտարածքի անվտանգության պատասխանատուն է Բելառուսի ներքին գործերի նախարարության բարձր տեխնոլոգիաների հանցագործությունների բաժինը:[110]

ՎՐԱՍՏԱՆ

Վրաստանում դեռևս ազգային անվտանգության 2011 թվականի հայեցակարգով արդեն արձանագրվեց, որ «տեղեկատվական համակարգում» պետական քաղաքականության պասիվությունը կարող է հանգեցնել «արտաքին ուժերի կողմից» Վրաստանի նկատմամբ հարձակումների:[111] 2014 թվականի ազգային ռազմական ռազմավարությամբ կիբեռվտանգները դասվում են

[107] Беларусь и Россия обсудили проект Концепции информационной безопасности Союзного государства, Белта, 13.04.2022, по ссылке: https://www.belta.by/politics/view/belarus-i-rossija-obsudili-proekt-kontseptsii-informatsionnoj-bezopasnosti-sojuznogo-gosudarstva-495901-2022/.

[108] Военный информационный портал, Министерство обороны Республики Беларусь (назначение войск радиоэлектронной борьбы), по ссылке: https://www.mil.by/ru/forces/special/reb/appointment/.

[109] Военный информационный портал, Министерство обороны Республики Беларусь (история войск радиоэлектронной борьбы), по ссылке: https://www.mil.by/ru/forces/special/reb/history/.

[110] Cyber Policy Portal, UNIDIR, page on Belarus last reviewed in June 2022, at: https://cyberpolicyportal.org/states/belarus

[111] Концепция национальной безопасноти Грузии, 2011, по ссылке: https://constitutions.ru/?p=5249.

պետության անվտանգության դեմ 5 հիմնական ռիսկերի շարքին:[112] 2021 թվականին Վրաստանում կառավարության կողմից հաստատվել է պաշտպանության նախարարության 2021-2024 թվականների համար կիբեռանվտանգության ազգային ռազմավարությունը և դրա գործողությունների ծրագիրը: Ըստ հասանելի տեղեկությունների՝ ռազմավարությամբ ընդգծվում է վտանգների երկու հիմնական խումբ՝ 1) կիբեռպատերազմը (ներառյալ՝ տեղեկատվական պատերազմը, կիբեռլրտեսությունը, պետությունների կողմից իրականացվող կիբեռհարձակումները) և 2) կիբեռհանցավորությունը (ներառյալ՝ կրիտիկական կարևորություն ունեցող ենթակառուցվածքների վրա հարձակումները):[113] Այլ կերպ ասած՝ Վրաստանի 2021 թվականի վերոհիշյալ ռազմավարությամբ կարգավորվում է երկրի կիբեռպաշտպանությունն ու կիբեռանվտանգությունը: Ընդ որում, ինստիտուցիոնալ առումով ռազմավարության իրականացման պատասխանատուն է Վրաստանի պաշտպանության նախարարության համակարգում գործող կիբեռանվտանգության բյուրոն՝ հանրային իրավունքի իրավաբանական անձը: Վրաստանի կիբեռանվտանգության բյուրոն օժտված է նաև կիբեռպաշտպանության և կիբեռանվտանգության ոլորտում պետական քաղաքականությունը կատարելագործելու, ռազմավարական փաստաթղթեր և օրենսդրական ակտեր մշակելու իրավասությամբ:[114]

ՂԱԶԱԽՍՏԱՆ

Ղազախստանում 2017 թվականից գործում է «Ղազախստանի կիբեռվահան» ազգային ռազմավարությունն ու դրա հիման վրա գործողությունների ծրագիրը, [115] իսկ 2022-2027 թվականներին Ղազախստանում գործելու է «Կիբեռվահան 2» լրամշակված ծրագիրը, որն ըստ հրապարակային տեղեկությունների՝ առավելապես ուղղված է կիբեռհանցագործությունների կանխարգելմանը, ինչպես նաև

[112] Cyber Policy Portal, UNIDIR, page on Georgia last reviewed in May 2022, at: https://cyberpolicyportal.org/states/georgia.
[113] В Грузии утверждена национальная стратегия кибербезопасности, 07.10.2021, по ссылке: https://civil.ge/ru/archives/446864.
[114] Ministry of Defense of Georgia official web-page, Cyber Security Bureau home page, at: https://mod.gov.ge/en/page/59/cyber-security-bureau.
[115] Об утверждении Концепции кибербезопасности ("Киберщит Казахстана") Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407, по ссылке: https://adilet.zan.kz/rus/docs/P1700000407.

համակարգչային միջադեպերի կառավարմանը:[116] Այլ կերպ ասած՝ կիբեռտարածքի ռազմական օգտագործման գործոնը բավարար կարգավորված չէ ռազմավարական մակարդակով:

Ինստիտուցիոնալ առումով Ղազախստանում թվային տեխնոլոգիաների զարգացման և վիրտուալ տիրույթի անվտանգության ոլորտում համակարգումն իրականացնում է թվային զարգացման, նորարարությունների և օդատիեզերական արդյունաբերության նախարարությունը: Մինչդեռ համակարգչային միջադեպերին արձագանքման նպատակով Ղազախստանում ստեղծվել է Համակարգչային միջադեպերին արձագանքելու ծառայություն:[117]

ՂՐՂԶՍՏԱՆ

Ղրղզստանում 2019 թվականին ընդունվել է Ղրղզստանի «Տեղեկատվական անվտանգության 2019-2023 թվականների ռազմավարությունը», որը կազմում է պետության ազգային անվտանգության բաղկացուցիչ տարրը:[118] Ռազմավարության շրջանակում որպես արդի ռիսկեր են դիտարկվում, մասնավորապես, տեղեկատվական քարոզչությունն ու էքսպանսիան, կիբեռտիրույթի էքստրեմիստական և ահաբեկչական նպատակներով օգտագործումը, կիբեռհանցանքները (այդ թվում՝ անդրազգային), ինտերնետի օգտագործումը տարբեր ոլորտներում պետության ներքին քաղաքականության վրա ներազդելու համար:[119] Ռազմավարությամբ սահմանված ռիսկերի վերլուծությունից կարելի է եզրահանգել, որ պետության պաշտպանության ոլորտում կիբեռտարածքի նշանակությունն ու առկա ռիսկերը, ըստ էության, անտեսված են:[120] Կիբեռոլորտում

---

[116] В 2022 году будет принята новая редакция концепции «Киберщит Казахстана», 31.03.2022, по ссылке: https://kz.kursiv.media/2022-03-31/v-2022-godu-budet-prinyata-novaya-redakciya-koncepcii-kibershhit-kazahstana/; В Казахстане запускают “Киберщит-2”, 28.07.2022, по ссылке: https://kazislam.kz/v-kazahstane-zapuskayut-kibershhit-2/.

[117] Служба реагирования на компьютерные инциденты, официальная веб-страница по ссылке: https://www.cert.gov.kz/.

[118] Приложение к постановлению Правительства Кыргызской Республики от 3 мая 2019 года № 209, Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы, по ссылке: http://cbd.minjust.gov.kg/act/view/ru-ru/13652.

[119] *Ibid.*, пункты 12-15, 31-33.

[120] Կիբեռտարածքի հնարավոր ռազմական օգտագործմանը վերացական անդրադարձ է կատարվում միայն ռազմավարության 40-րդ կետի 3-րդ ենթակետում և 45-րդ կետում:

Ղրղզստանի մնացած ռազմավարական փաստաթղթերն առավելապես ուղղված են թվայնացման զարգացման հարցերին:[121]

Ինստիտուցիոնալ տեսանկյունից Ղրղզստանում կիբեռոլորտի համակարգումն իրականացնում է Ղրղզստանի Հանրապետության թվային տեխնոլոգիաների և կապի պետական կոմիտեն,[122] ինչպես նաև Ազգային անվտանգության ազգային կոմիտեի կիբեռանվտանգության ապահովման համակարգման կենտրոնը[123]: 2021 թվականին տարածված հաղորդագրության համաձայն՝ պետական-մասնավոր համագործակցության արդյունքում ծրագրվում է ստեղծել «Ղրղզստանի կիբեռվահան»:[124]

ՏԱՋԻԿՍՏԱՆ

Տաջիկստանում կիբեռտարածքում անվտանգության ապահովումը թույլ դիրքեր ունի, կիբեռտարածքի ռազմական օգտագործումն առհասարակ անտեսված է, իսկ համապատասխան արդի ռազմավարական փաստաթղթերը, ըստ հրապարակային տվյալների, բացակում են:[125] 2016 թվականին Տաջիկստանում ընդունվել է Տաջիկստանի Հանրապետության զարգացման ազգային ծրագիրը մինչև 2030

---

[121] Программа цифровой трансформации Киргизии «Таза Коом», 20.01.2018, по ссылке: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A2%D0%B0%D0%B7%D0%B0_%D0%9A%D0%BE%D0%BE%D0%BC_(%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%82%D1%80%D0%B0%D0%BD%D1%81%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8_%D0%9A%D0%B8%D1%80%D0%B3%D0%B8%D0%B7%D0%B8%D0%B8); Указ Президента Кыргызской Республики от 12 октября 2021 года УП № 435 "О национальной программе развития Кыргызской Республики до 2026 года", по ссылке: http://cbd.minjust.gov.kg/act/view/ru-ru/430699.

[122] Положение о Государственной службе цифрового развития при Правительстве Кыргызской Республики, Приложение 1 к постановлению Правительства Кыргызской Республики от 10 марта 2021 года № 86, по ссылке: http://cbd.minjust.gov.kg/act/view/ru-ru/158168?cl=ru-ru.

[123] Положение о Координационном центре по обеспечению кибербезопасности Государственного комитета национальной безопасности Кыргызской Республики, по ссылке: https://gknb.kg/%D0%BA%D1%86%D0%BA%D0%B1-%D0%B3%D0%BA%D0%BD%D0%B1-%D0%BA%D1%80/.

[124] В Кыргызстане будет создан киберщит по обеспечению кибербезопасности, VESTI.KG - Новости Кыргызстана, 11.09.2021, по ссылке: https://vesti.kg/obshchestvo/item/90654-v-kyrgyzstane-budet-sozdan-kibershchit-po-obespecheniyu-kiberbezopasnosti.html.

[125] Վերջին ռազմավարական փաստաթուղթը 2003 թվականի Տեղեկատվական անվտանգության մասին ռազմավարությունն է, տես՝ http://www.adlia.tj/spisdoc.fwx?sortord=dat_dok+desc&startpage=1&razdel=1&kl_slova=&gde_slova=&filter=_410010000&vdd=13010&nqtype=2&dtype=0&year=2015&select_format=2&login=yes.

թվականը, որտեղ, սակայն, միայն մակերեսային անդրադարձ է կատարվում տեղեկատվական տեխնոլոգիաների ներդրման և զարգացման անհրաժեշտությանը՝ առանց անդրադառնալու անվտանգային և, առավել ևս, պաշտպանական բաղադրիչներին:[126] Վերոհիշյալ պատկերը բնականաբար հայելակերպ արտացոլված է նաև Տաջիկստանի կիբեռտարածքի կարգավորման ինստիտուցիոնալ մակարդակում:

ՈՒԶԲԵԿՍՏԱՆ

Ուզբեկստանում 2020 թվականին ծրագրվեց մշակել կիբեռանվտանգության ազգային ռազմավարություն 2020-2023 թվականների համար, որի հիմքով նախատեսվում էր ընդունել նաև կիբեռպաշտպանության ոլորտում օրենք:[127] 2022 թվականին Ուզբեկստանում ընդունվել է կիբեռանվտանգության մասին օրենքը, որն առայժմ ուժի մեջ չի մտել:[128] Հիշյալ օրենքն ուղղված է կարգավորելու կիբեռտարածքի անվտանգության ապահովումը, ներառյալ՝ պաշտպանության բնագավառում կրիտիկական տեղեկատվական օբյեկտների անվտանգությունը: Օրենքով անդրադարձ չի կատարվում կիբեռտարածքի ռազմական կիրառության կարգավորմանը:[129] Կիբեռանվտանգության ոլորտում Ուզբեկստանի այլ իրավական փաստաթղթերը (ինչպես, օրինակ, Ուզբեկստանի Հանրապետության նախագահի որոշումը՝ տեղեկատվական տեխնոլոգիաների և հաղորդակցության ներդրման վերահսկման, կազմակերպման և պաշտպանության համակարգի կատարելագործմանն ուղղված միջոցառումների վերաբերյալ,[130] Ուզբեկստանի նախարարների կաբինետի որոշումը՝ «Ինտերնետում տեղեկատվական

---

[126] Национальная стратегия развития Республики Таджикистан на период до 2030 года, Утверждена постановлением Маджлиси намояндагон Маджлиси Оли Республики Таджикистан от 1 декабря 2016 года, N 636, по ссылке: https://medt.tj/documents/main/strategic_national_programm/strategic_national_prog_ru.pdf.

[127] «Узбекистан задумался о кибербезопасности», 11. 02. 2020, по ссылке: https://www.gazeta.uz/ru/2020/02/11/cybersecurity/.

[128] Закон Республики Узбекистан «О кибербезопасности», принят Законодательной палатой 25.02.2022, одобрен Сенатом 17.03.2022, по ссылке: https://lex.uz/uz/docs/5960609.

[129] «Узбекистан задумался о кибербезопасности», supra n. 127.

[130] Постановление Президента Республики Узбекистан 21.11.2018 г. ПП-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты», по ссылке: https://nrm.uz/contentf?doc=568218_postanovlenie_prezidenta_respubliki_uzbekistan_ot_21_11_2018_g_n_pp-4024_o_merah_po_sovershenstvovaniyu_sistemy_kontrolya_za_vnedreniem_informacionnyh_tehnologiy_i_kommunikaciy_organizacii_ih_zashchity&products=1_vse_zakonodatelstvo_uzbekistana.

անվտանգության կատարելագործմանն ուղղված միջոցառումների մասին»[131]) նույնպես չեն կարգավորում կիբեռտարածքի ռազմական օգտագործման խնդիրները: Կիբեռանվտանգության ապահովման գործառույթն Ուզբեկստանում համապատասխանաբար համակարգում է տեղեկատվական տեխնոլոգիաների և հաղորդակցության զարգացման նախարարությունը: Միևնույն ժամանակ, Ուզբեկստանի Հանրապետության նախագահի որոշմամբ՝ տեղեկատվական տեխնոլոգիաների և հաղորդակցության ներդրման վերահսկման, կազմակերպման և պաշտպանության համակարգի կատարելագործմանն ուղղված միջոցառումների վերաբերյալ որոշման հիման վրա գործում է Կիբեռանվտանգության կենտրոնը:[132]

ԹՈՒՐՔՄԵՆՍՏԱՆ

Թուրքմենստանում 2022 թվականին հաստատվել է կիբեռանվտանգության ռազմավարությունը 2022-2025 թվականների համար, որն ըստ հրապարակային հաղորդագրությունների՝ ուղղված է լինելու կիբեռհանցանքների կանխարգելմանը:[133] Հայտնի է նաև, որ Թուրքմենստանի զինված ուժերում իրականացվում է «կիբեռտարածքի զորքերի» նախապատրաստում, իսկ, մասնավորապես, 2018-2019 թթ. ուսումնական տարում Թուրքմենստանի պաշտպանության նախարարության ռազմական ինստիտուտում բացվել է նման մասնագետների նախապատրաստման առանձին կուրս:[134] Մինչդեռ ոչ ռազմական բնագավառում կիբեռանվտանգության ոլորտում լիազորություններով օժտված է, մասնավորապես, Թուրքմենստանի նախարարների կաբինետի տրանսպորտի և հաղորդակցության գործակալությունը:

---

[131] Постановление Кабинета министров Республики Узбекистан от 05.09.2018 г. N 707 "О мерах по совершенствованию информационной безопасности во всемирной информационной сети Интернет", https://nrm.uz/contentf?doc=556002_postanovlenie_kabineta_ministrov_respubliki_uzbekistan_ot_05_09_2018_g_n_707_o_merah_po_sovershenstvovaniyu_informacionnoy_bezopasnosti_vo_vsemirnoy_informacionnoy_seti_internet&products=1_vse_zakonodatelstvo_uzbekistana.

[132] Государственное унитарное предприятие Центр кибербезопасности, официальная веб-страница по ссылке: https://tace.uz/ru/company/.

[133] Утверждена Госпрограмма обеспечения кибербезопасности Туркменистана, Turkmenportal, 02.03.2022, по ссылке: https://turkmenportal.com/blog/44862/utverzhdena-gosprogramma-obespecheniya-kiberbezopasnosti-turkmenistana.

[134] В Туркменистане начали готовить военных специалистов по кибербезопасности», SNG.FM, 2018, по ссылке: https://sng.fm/11487-v-turkmenistane-nachali-gotovit-voennyh-specialistov-po-kiberbezopasnosti.html.

ՈՒԿՐԱԻՆԱ

Ուկրաինայում մինչև 2021 թվականը գործում էր Ուկրաինայի ազգային անվտանգության և պաշտպանության խորհրդի կողմից ներկայացված և 2016 թվականին հաստատված կիբեռանվտանգության ռազմավարությունը, որը 2021 թվականին Ուկրաինայի նախագահի հրամանագրով ճանաչվեց ուժը կորցրած՝ կիրառության մեջ դնելով կիբեռանվտանգության նոր ռազմավարությունը,[135] որի իրականացման գործողությունների ծրագիրը գործողության մեջ է դրվել 2022 թվականի փետրվարին[136]: Կիբեռանվտանգության նոր ռազմավարության հիմնական կարևոր ուղղություններից է սահմանվել նաև կիբեռտարածքի ռազմական օգտագործման համատեքստում արդյունավետ կիբեռպաշտպանության ձևավորումն ու զարգացումը, իսկ ռազմավարության և դրանից բխող գործողությունների ծրագրի իրականացման պարտականությունը դրվել է Կիբեռանվտանգության համակարգման ազգային կենտրոնի վրա:[137]

ՄՈԼԴՈՎԱ

Մոլդովայում 2018 թվականի նոյեմբերին հաստատվեց Մոլդովայի Հանրապետության տեղեկատվական անվտանգության 2019-2024 թվականների ռազմավարությունը և դրա իրականացման գործողությունների ծրագիրը: Ռազմավարությամբ հաստատվում է կիբեռտարածքի ռազմական օգտագործման պոտենցիալն ու նոր իրողությունները՝ որպես ռազմավարության կարևոր հիմնասյուն սահմանելով կիբեռպաշտպանության գործառնական կարողությունների ամրապնդումը:[138] Այս համատեքստում ռազմավարության նախապատվություններից է արձանագրված կիբեռպաշտպանության ապահովման նպատակով Մոլդովայի զինված ուժերում առանձին կառուցվածքային ստորաբաժանման ստեղծումը:[139] Հարկ է ընդգծել, որ զինված կիբեռհարձակումներից պաշտպանությունը

---

[135] Зеленский утвердил обновленную Стратегию кибербезопасности Украины, Интерфакс-Украина, 26.08.2021, по ссылке: https://interfax.com.ua/news/general/764179.html.

[136] Страна теперь будет реализовывать Стратегию кибербезопасности, ZN'UA, 02.02. 2022, https://zn.ua/POLITICS/zelenskij-podpisal-ukaz-o-reshenii-snbo-v-sfere-kiberbezopasnosti.html.

[137] Ukraine President adopts Cyber Security Strategy Implementation Plan, DataGuidance, 03.02.2022, at: https://www.dataguidance.com/news/ukraine-president-adopts-cyber-%E2%80%8B%E2%80%8Bsecurity-strategy.

[138] Lisnic Sergiu, Center for Combating Cyber Crimes of NII of GIP, Republic of Moldova, Information security strategy of the Republic of Moldova for 2019-2024 and the Plan of actions for its implementation, at: https://rm.coe.int/3-moldova-strategy/168097eceb.

[139] Lisnic Sergiu, *ibid*.

կազմակերպելու կարողությունների շարունակական զարգացումն ամրագրված էր նաև Մոլդովայի 2018-2021 թվականների ազգային պաշտպանության ռազմավարությամբ:[140] 2021 թվականին Մոլդովայի Հանրապետության զինված ուժերի համակարգում ՆԱՏՕ-ի աջակցությամբ ձևավորվում է կիբեռպաշտպանության հատուկ ենթակառուցվածք՝ Մոլդովայի Հանրապետության զինված ուժերի կիբեռարձագանքման կարողություններ:[141]

ՌՈՒՍԱՍՏԱՆԻ ԴԱՇՆՈՒԹՅՈՒՆ

Ռազմական կիբեռպաշտպանության հիմքերը Ռուսաստանում ամրագրված են ՌԴ 2010 թվականի ռազմական դոկտրինում,[142] 2021 թվականի ՌԴ ազգային անվտանգության ռազմավարությունում,[143] կրիտիկական տեղեկատվական ենթակառուցվածքների պաշտպանությանն ուղղված ՌԴ օրենսդրությամբ[144]: 2017 թվականին ՌԴ պաշտպանության նախարարության համակարգում ձևավորվել է կիբեռօպերացիաների իրականացման ստորաբաժանում, սակայն պաշտպանության նախարարի պաշտոնական հայտարարության համաձայն՝ նշված ստորաբաժանումը առավելապես ներգրավված է ռազմական քարոզչության և հակաքարոզչության իրականացման աշխատանքներում,[145] ինչը չի կարող նույնացվել կիբեռտարածքում ռազմական օպերացիաների ոլորտում գործունեության հետ: Մինչդեռ ավանդական իմաստով կիբեռզորքեր ձևավորելու վերաբերյալ քննարկումներ տեղի են ունեցել

[140] Cyber Policy Portal, UNIDIR, page on Republic of Moldova last reviewed in May 2022, at: https://cyberpolicyportal.org/states/republic-of-moldova.

[141] The NATO Science for Peace and Security (SPS) Programme, Inauguration of the Moldovan Armed Forces Cyber Incident Response Capability, 21.01.2021, at: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/2/pdf/210208-sps-moldovan-brochure.pdf, в Республике Молдова при поддержке НАТО создан потенциал реагирования на киберинциденты, 21.01.2021, по ссылке: https://www.nato.int/cps/ru/natohq/news_180758.htm?selectedLocale=ru.

[142] Военная доктрина Российской Федерации от 05. 02. 2010 (утверждена Указом Президента Российской Федерации), пп. 12.1, 13.г), 15, 41.в) и г), по ссылке: http://kremlin.ru/supplement/461.

[143] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», п.17, по ссылке: http://www.kremlin.ru/acts/bank/47046.

[144] Президент России подписал разработанные Правительством Федеральные законы об обеспечении безопасности критической информационной инфраструктуры, 27. 07. 2017, по ссылке: http://government.ru/activities/selection/525/28727/.

[145] В Минобороны РФ создали войска информационных операций, Интерфакс, 22. 02. 2017, по ссылке: https://www.interfax.ru/russia/551054.

ՌԴ-ում 2022 թվականի մարտին:[146] Այսպիսով, առկա ռազմավարական փաստաթղթերի և տեղեկատվության վերլուծությունից կարելի է եզրահանգել, որ ՌԴ-ում ռազմական կիբեռպաշտպանության և ռազմական կիբեռպոտենցիալի օգտագործման ուղղությամբ բավարար քայլեր առայժմ արված չեն:

ԱԴՐԲԵՋԱՆ

Հրապարակային տեղեկությունների համաձայն՝ Ադրբեջանում 2014-2020 թվականներին գործել է Տեղեկատվական հասարակության զարգացման ազգային ռազմավարությունը, որի հիմնական խնդիրներից էր կիբեռանվտանգության և տեղեկատվական հասարակության զարգացման համար տեղեկատվական անվտանգության և ավանդական տնտեսական սեկտորների զարգացման ապահովումը:[147] 2018 թվականին ընդունվել է Ադրբեջանի նախագահի կարգադրությունը «Տեղեկատվական անվտանգության համակարգման հանձնաժողովի ստեղծման մասին», իսկ 2021 թվականին Ադրբեջանի նախագահի հրամանագիրը՝ «Կրիտիկական տեղեկատվական ենթակառուցվածքի անվտանգության ապահովման համար կոնկրետ միջոցառումներ ձեռնարկելու վերաբերյալ»:[148] 2022 թվականի փետրվարին տարածված հաղորդագրության համաձայն՝ Թվային զարգացման և տրանսպորտի փոխնախարար Ռովշան Ռուստամովը «Ապատեղեկատվության ցանցը և Ադրբեջանին սպառնացող հիբրիդային վտանգները» խորագրով փաստաթղթի քննարկման ժամանակ հայտարարել է, որ Ադրբեջանն արդեն մշակել է կիբեռանվտանգության պաշտպանության նոր ռազմավարություն:[149] Ադրբեջանն ակտիվորեն մասնակցում է ՆԱՏՕ-ի «Գիտությունը խաղաղության և անվտանգության համար» ծրագրին, մասնավորապես՝ կիբեռպաշտպանության ոլորտում:[150] 2022 թվականի հուլիսին հայտնի դարձավ նաև, որ Ադրբեջանի թվային զարգացման և տրանսպորտի նախարարության և Իսրայելի «Տեխնիոն» տեխնոլոգիական ինստիտուտի միջև կնքվել է համաձայնագիր, որով նախատեսվում է Ադրբեջանում ստեղծել

[146] В Минпромторге предложили создать в России кибервойска, РБК, 22. 03. 2022, по ссылке: https://www.rbc.ru/politics/22/03/2022/6239c7da9a7947db406ee240.
[147] Cyber Policy Portal, UNIDIR, page on Azerbaijan last reviewed in June 2022, at: https://cyberpolicyportal.org/states/azerbaijan.
[148] *Ibid.*
[149] Azerbaijan's cyber security strategy developed, Report news agency, 14 February 2022, at: https://report.az/en/ict/azerbaijan-s-cyber-security-strategy-developed/.
[150] NATO science for piece and security programme, country flyer for Azerbaijan 2021, at: https://www.nato.int/science/country-fliers/Azerbaijan.pdf.

կիբեռանվտանգության կենտրոն և առաջիկա երեք տարիների ընթացքում իրականացնել ավելի քան 1000 մասնագետների վերապատրաստում:[151] Ադրբեջանում նմանօրինակ կենտրոնի առկայությունը լրացուցիչ լուրջ մարտահրավեր է Հայաստանի համար՝ հաշվի առնելով նաև Ադրբեջանի և Թուրքիայի կիբեռկայացածության բարձր մակարդակը և վերջիններիս ռազմավարական-ռազմական համագործակցությունը:

2020 թվականի համաշխարհային կիբեռանվտանգության ինդեքսի հրապարակած տվյալների համաձայն՝ Ադրբեջանի գնահատականը 89,31 է, և այն քառասուներորդն է կիբեռանվտանգության հուսալիության տեսանկյունից:[152] Իսկ ազգային կիբեռանվտանգության ինդեքսով 2020 թվականի դրությամբ Ադրբեջանն այլ պետությունների շարքում 85-րդն է՝ ունենալով բավարար ցածր ցուցանիշ կիբեռանվտանգության քաղաքականության մշակման առումով (29%), բարձր ցուցանիշ կիբեռտարածքում վտանգների վերլուծության տեսանկյունից (80%), բարձր ցուցանիշ կրթության և մասնագիտական զարգացման տեսանկյունից (67%), բավարար ցածր ցուցանիշ կիբեռտարածքում ճգնաժամի կառավարման տեսանկյունից (20%) և նվազագույն զրոյական ցուցանիշ ռազմական ոլորտում կիբեռօպերացիաների կազմակերպման կարողությունների տեսանկյունից (0%):[153]

Կիբեռպաշտպանության ռազմավարական և ինստիտուցիոնալ կարգավորման ԱՊՀ տարածքի պետությունների փորձի վերլուծության հիմնական եզրահանգումները

Կիբեռանվտանգության և կիբեռպաշտպանության բնագավառում ԱՊՀ երկրների ռազմավարական փաստաթղթերի ուսումնասիրությունը թույլ է տալիս եզրակացնել, որ ուսումնասիրված գրեթե բոլոր երկրներում գործում են կիբեռանվտանգության ոլորտում ռազմավարական փաստաթղթեր և իրավական ակտեր, ապահովվում է ռազմավարական փաստաթղթերի շարունակական կատարելագործման գործընթացը: Միևնույն ժամանակ, ռազմական կիբեռպաշտպանության բնագավառում ռազմավարական փաստաթղթերի և ինստիտուցիոնալ համակարգի վերլուծությունը վկայում է, որ բացի Վրաստանից, Ուկրաինայից և Մոլդովայից, մյուս պետությունները ռազմավարական

[151] Azerbaijan, together with Israel, creates a center of cybersecurity, Silkway News, 1 July 2022, at: https://www.silkway.news/azerbaijan-together-with-israel-creates-80302/.
[152] Global Cybersecurity Index 2020, supra n. 74.
[153] NCSI for Azerbaijan, at: https://ncsi.ega.ee/country/az/.

մակարդակում չեն կարգավորում կիբեռտարածքի ռազմական օգտագործմանը վերաբերող խնդիրները՝ լավագույն դեպքում սահմանափակվելով կրիտիկական ենթակառուցվածքների պաշտպանության և կիբեռմիջադեպերի արձագանքման կառուցակարգերի սահմանմամբ: Ուսումնասիրված երկրներից, թեև Ադրբեջանում ռազմավարական մակարդակում ռազմական կիբեռպաշտպանության կարգավորման վերաբերյալ հրապարակային տեղեկությունները բացակայում են, այնուամենայնիվ, հատկանշական է, որ Ադրբեջանը՝ համագործակցելով ՆԱՏՕ-ի հետ ՆԱՏՕ-ի «Գիտությունը խաղաղության և անվտանգության համար» ծրագրի շրջանակում, ինչպես նաև Իսրայելի «Տեխնիոն» տեխնոլոգիական ինստիտուտի հետ համագործակցությամբ, ձեռնարկում է գործուն պրակտիկ միջոցառումներ պետության ռազմական կիբեռկարողությունների զարգացման ուղղությամբ:

Հետաքրքրական է նաև այսպես կոչված «արևմուտքի երկրների» և ԱՊՀ տարածաշրջանի երկրների կողմից ռազմավարական մակարդակում տվյալ հարցի համատեքստում օգտագործվող տերմինաբանական տարբերությունը՝ ԱՊՀ երկրներում «կիբեռանվտանգության» փոխարեն «տեղեկատվական անվտանգության» հայեցակարգի գերակայությամբ, ինչպես նաև կիբեռպատերազմի ռազմական քարոզչության, կամ հիբրիդային-տեղեկատվական օպերացիաների հետ նույնացման միտումով: Նշվածն ինքին վկայում է այն մասին, որ ռազմավարական մակարդակում բացակայում է պետության ռազմական կիբեռպաշտպանության ձևավորված տեսլական:

Կիբեռպաշտպանության ռազմավարական և ինստիտուցիոնալ կարգավորումները Հայաստանի Հանրապետությունում

Հաշվի առնելով Արցախի Հանրապետության անվտանգության և արտաքին թշնամուց պաշտպանության խնդիրները, Հայաստանի Հանրապետության անվտանգության և տարածքային ամբողջականության նկատմամբ իրական սպառնալիքները, ինչպես նաև Հայաստանի Հանրապետության համար ստեղծված երկարաժամկետ տարածաշրջանային բարդ իրադրությունը՝ վերջին տասնամյակների ընթացքում Ադրբեջանի կողմից պարբերաբար կրկնվող զինված հարձակումները Արցախի Հանրապետության ուղղությամբ, Ադրբեջանի և Թուրքիայի իրականացրած ագրեսիան Հայաստանի Հանրապետության դեմ և դրա շարունակական դրսևորման հավանականությունն ու սպառնալիքները՝ անվիճելի է, որ Հայաստանի Հանրապետության պետական քաղաքականության առանցքային

խնդիրներից բոլոր ժամանակներում պետք է լիներ և ներկայումս էլ պետք է որպես առաջնահերթություն դիտարկվի ազգային անվտանգության և պետական պաշտպանության հստակ, իրագործելի, չափելի, բովանդակալից և պատեհաժամ ռազմավարությունների առկայությունը, որոնք պետք է ներառեին տարբեր բնագավառներում առկա խնդիրների և արդի մարտահրավերների վերլուծությունը, Հայաստանի Հանրապետության պետական քաղաքականության հիմնական ուղղությունները և դրա իրականացմանն ուղղված բովանդակային դրույթներ:

Անվիճելի է նաև, որ 21-րդ դարում տեղեկատվական անվտանգությունը, կիբեռանվտանգությունը և կիբեռպաշտպանությունը ազգային անվտանգության և պետական պաշտպանության կարևորագույն բաղկացուցիչ տարր են, իսկ տվյալ ուղղություններով համապարփակ հայեցակարգային փաստաթղթերի մշակումն ու իրագործումը (ներառյալ՝ պարբերաբար դրանց վերանայումն ու լրամշակումը) նշված ոլորտների արդյունավետ կառավարման ու պետության պաշտպանության և անվտանգության ապահովման համար անփոխարինելի միջոցներ են: Այս հարցի շուրջ իրականացրած վերլուծությունը հանգեցնում է ցավալի եզրահանգումների:

Հայաստանում այսօր մարդկանց կենսունակության և կառավարության գործունեության բոլոր ասպեկտները, ներառյալ՝ այնպիսի տարբեր ոլորտներում կրիտիկական ենթակառուցվածքները, ինչպիսիք են հեռահաղորդակցությունը, էներգետիկան, բանկային և ֆինանսական համակարգերը, ռազմական ոլորտը, տրանսպորտային ենթակառուցվածքները, ավիացիոն համակարգը, ջրամատակարարման համակարգը, արտակարգ իրավիճակներում օգնություն ցուցաբերելու ծառայությունները և կենսապահովման այլ համակարգեր, ըստ էության, սերտորեն փոխկապակցված են և շատ դեպքերում հիմնված են համակարգչային համակարգերի վրա: Ենթակառուցվածքների (այդ թվում՝ կրիտիկական ենթակառուցվածքների) սերտ փոխկապակցվածության, ինչպես նաև համակարգչային համակարգերից դրանց կախվածության արդյունքում մեծանում է ռազմական կիբեռհարձակումների ռիսկը և հրամայական է դառնում ամուր կիբեռպաշտպանություն կազմակերպելը, ներառյալ, բայց չսահմանափակվելով կրիտիկական ենթակառուցվածքների սահմանմամբ և պաշտպանությամբ: Հենց տվյալ ոլորտում առկա և օրեցօր մեծացող վտանգներն են, որ շատ պետությունների (հատկապես այն պետությունների, որոնք ներքաշված են կամ մեծ հավանականությամբ կարող են ներքաշվել ռազմական հակամարտությունների մեջ) ստիպում են օրակարգում գերակայող հարց դարձնել կիբեռանվտանգության և

ռազմական կիբեռպաշտպանության ապահովման ուժեղ և արդյունավետ հայեցակարգի, ռազմավարության, ծրագրի և գործողությունների պլանի մշակումը և կիրառումը:

Ռազմական բնագավառում պաշտպանական գործողություններ (պատասխան հարձակումներ) իրականացնելու արդյունավետությունն ապահովելու նպատակով կիբեռմիջոցների օգտագործումը իրենից ներկայացնում է նոր տեխնոլոգիաների ամենագրավիչ հնարավորություններից մեկը, որի ռացիոնալությունը և մատչելիությունը պայմանավորված են նվազագույն ծախսերով և առավելագույն արդյունքների հասնելու ներուժով:

Կիբեռպաշտպանության ռազմավարական և ինստիտուցիոնալ կարգավորումները ՀՀ-ում 2000-2018թթ.

Հայաստանի Հանրապետությունը տեղեկատվական անվտանգության և «էլեկտրոնային հասարակության» ձևավորման ու զարգացման ապահովման ոլորտում կոնկրետ միջոցները սկսել է ձեռնարկել արդեն 2000-ական թվականների առաջին տասնամյակում: Այսպես, 2001 թվականին ստորագրվեց, 2006 թվականին ռատիֆիկացվեց և 2007 թվականին ուժի մեջ մտավ «Կիբեռհանցագործությունների մասին» 2001 թվականի Բուդապեշտի կոնվենցիան:[154]

2008 թվականի մարտի 13-ին ՀՀ կառավարության որոշմամբ հաստատվեց տեղեկատվական տեխնոլոգիաների ոլորտի զարգացման պետական աջակցության 2008 թվականի ծրագիրը,[155] որը նպատակ էր հետապնդում նպաստել՝ 1) տեղեկատվական տեխնոլոգիաների ոլորտի ներկա իրավիճակի վերլուծության հետազոտությունների իրականացմանը, 2) ՀՀ տեղեկատվական տեխնոլոգիաների ոլորտում ձեռքբերումները միջազգային և տեղական հարթակներում ներկայացնելուն,

3) տվյալ ոլորտում միջազգային համագործակցության զարգացմանը և 4) ՀՀ-ում կայուն զարգացման համատեքստում իրավիճակի բարելավմանը: Հարկ է ընդգծել, որ տվյալ փաստաթղթով կիբեռանվտանգության կամ կիբեռպաշտպանության վերաբերյալ որևէ դրույթ նախատեսված չէ:

---

[154] «Կիբեռհանցագործությունների մասին» 2001 թվականի Բուդապեշտի կոնվենցիա, տես՝ https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185:

[155] ՀՀ կառավարության 2008 թվականի մարտի 13-ի N 293-Ն որոշումը «Տեղեկատվական տեխնոլոգիաների ոլորտի զարգացման պետական աջակցության 2008 թվականի ծրագիրը հաստատելու մասին»:

2009 թվականին ընդունվեցին հետևյալ հիմնական փաստաթղթերը.

- ՀՀ նախագահի կարգադրությունը «ՀՀ տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին» (այսուհետ նաև՝ ՏԱ հայեցակարգ),[156] որն ուժը կորցրել է նախագահի 2017 թվականի նոյեմբերի 11-ին ՆԿ-97-Ն կարգադրությամբ,
- ՀՀ նախագահի կարգադրությունը «ՀՀ տեղեկատվական անվտանգության հայեցակարգի դրույթներով նախատեսված ծրագրերի իրականացումը համակարգող միջգերատեսչական հանձնաժողով ստեղծելու մասին» (ուժը կորցրել է 05.04.18թ. ՀՀ նախագահի ՆԿ-49-Ն կարգադրությամբ),
- ՀՀ-ում էլեկտրոնային հասարակություն ստեղծելու հայեցակարգը (2010-2012),[157]
- ՀՀ վարչապետի «Կիբեռանվտանգության հարցերով պետական հանձնաժողով ստեղծելու, դրա կազմը և աշխատակարգը հաստատելու մասին» 2011թ. հունվարի 13-ի թիվ 14-Ա որոշումը[158]:

Նշենք, որ ՀՀ նախագահի 2009թ. հուլիսի 26-ի «ՀՀ տեղեկատվական անվտանգության մասին» հայեցակարգը հաստատելու մասին» կարգադրությունը Հայաստանի Հանրապետությունում պետական մակարդակում կիբեռանվտանգության ոլորտի առաջին պաշտոնական քայլերից էր: ՏԱ հայեցակարգը միտված էր տեղեկատվական անվտանգության ոլորտում պետական շահերի հիմնական բաղադրիչները որոշելուն և առաջադրված նպատակներին հասնելու հիմնական միջոցառումների կանոնակարգմանը, տեղեկատվական անվտանգության և դրա աղբյուրների հետ կապված սպառնալիքների հիմնական տեսակների նույնականացմանը, ՏԱ հայեցակարգի մշակման պահին ՀՀ-ում տեղեկատվական անվտանգության վիճակի նկարագրմանը և ՀՀ առանցքային խնդիրների վերհանմանը՝ տեղեկատվական անվտանգության և դրա կառուցակարգերի արդյունավետ իրականացումն ապահովելու համար, ըստ գործունեության ոլորտների (տնտեսական ոլորտ, ներքին և արտաքին քաղաքականության ոլորտներ, պաշտպանության, գիտության և տեխնիկայի,

[156] ՆԿ-97, ընդունվել է 26.06.2009, ուժի մեջ է մտել 25.07.2009:
[157] Հավելված ՀՀ կառավարության 2010թ. փետրվարի 25–ի նիստի N 7 արձանագրային որոշման:
[158] «Կիբեռանվտանգության հարցերով պետական հանձնաժողով ստեղծելու, դրա կազմը և աշխատակարգը հաստատելու մասին» թիվ 14-Ա որոշումը ընդունվել է 13.01.2011, ուժի մեջ է մտել 14.01.2011, ՀՀ վարչապետի որոշումը (N 175 - Ա) ՀՀ Վարչապետի 2011 թվականի հունվարի 13-ի N 14 – Ա որոշման մեջ փոփոխություն կատարելու և կիբեռանվտանգության պետական հանձնաժողովի անհատական կազմը հաստատելու մասին, ընդունվել է 09.03.2011, ուժի մեջ է մտել 10.03.2011:

արտակարգ իրավիճակների և այլ ոլորտներ) տեղեկատվական անվտանգության ապահովման առանձնահատկությունները որոշելուն, տեղեկատվական անվտանգության ապահովման ուղղությամբ պետական քաղաքականության հիմնական դրույթները և նշված քաղաքականության իրագործման գերակա միջոցառումները որոշելուն, ինչպես նաև տեղեկատվական անվտանգության ապահովումը կազմակերպելու հիմքերը կանոնակարգելուն:[159]

ՏԱ հայեցակարգի իրագործման համար ՀՀ նախագահը նաև ստորագրեց կարգադրություն միջգերատեսչական կոմիտեի ստեղծման մասին, որի կազմի մեջ ներառվել էին Ազգային անվտանգության խորհրդից, ՀՀ նախագահի աշխատակազմից, ՀՀ տրանսպորտի և կապի նախարարությունից, ՀՀ պաշտպանության նախարարությունից, ՀՀ արդարադատության նախարարությունից, ՀՀ կրթության և գիտության նախարարությունից, ՀՀ էկոնոմիկայի նախարարությունից, ՀՀ կառավարությանն առընթեր ազգային անվտանգության ծառայությունից և ՀՀ գիտությունների ազգային ակադեմիայից բարձրագույն պաշտոնատար անձինք:[160] Այս համատեքստում ուշադրության են արժանի մի շարք գործոններ՝

- ՏԱ հայեցակարգը և կոմիտեի կազմը հաստատվել էին ՀՀ նախագահի կողմից, ինչը նշանակում է, որ տեղեկատվական անվտանգությունն ապահովելու քաղաքականությունը գտնվում էր ՀՀ նախագահի անմիջական հսկողության ներքո: ՏԱ հայեցակարգը միտված էր *տեղեկատվական անվտանգության* ապահովմանը: Կարգավորման առարկայի շեշտադրումը կարևորվում է՝ հաշվի առնելով, որ «տեղեկատվական անվտանգություն» և «կիբեռանվտանգություն» հասկացություններին տեսությունում կարող է տրվել տարբեր նշանակություններ: Մասնավորապես, ընդունված է, որ «տեղեկատվական անվտանգություն» կատեգորիան ավելի լայն է, քան «կիբեռանվտանգությունը» և բացի կիբեռանվտանգության տարրերից, կարող է ներառել նաև, օրինակ, այնպիսի տարրեր, ինչպիսիք են՝ պետության տեղեկատվական քաղաքականության մշակումը կամ պետական քաղաքականության կամ պատմության մասին ԶԼՄ-ների միջոցով կամ այլ կերպ սուտ տեղեկությունների տարածման դեմ պայքարը[161]: [162]

---

[159] ՆԿ-97, Հավելված:

[160] ՆԿ-225-Ն, Հավելված 1:

[161] ՆԿ-97, Հավելված, II, էջեր 3-4:

[162] Հարկ է ընդգծել, որ տեղեկատվական անվտանգության և կիբեռանվտանգության ոլորտների արդյունավետ կառավարման համար էականորեն կարևոր է նշված հասկացությունների ճիշտ

- ՏԱ հայեցակարգը կարգավորում էր նաև պաշտպանության ոլորտում որոշակի ասպեկտներ,[163] որոնց կենսագործումն ապահովելու համար համապատասխան միջգերատեսչական կոմիտեի կազմում ներառվել էր պաշտպանության նախարարության ներկայացուցիչը: Դա վկայում է այն մասին, որ տեղեկատվական անվտանգության ապահովման ոլորտում հենց առաջին լուրջ քայլերն իրականացնելու պահից ընդունվել է տեղեկատվական անվտանգության և պետական պաշտպանության միջև հատուկ հարաբերակցության արդիականությունը:

Միևնույն ժամանակ, հատուկ հետաքրքրություն է ներկայացնում ՏԱ հայեցակարգի այն դրույթը, որով որպես ՀՀ միջազգային համագործակցության առանձին ուղղություն սահմանվում է «տեղեկատվական զենքի» մշակման, տարածման և կիրառման արգելքի անհրաժեշտությունը: [164] Ընդ որում, ելնելով համատեքստից, կարելի է եզրակացնել, որ հայեցակարգի «տեղեկատվական զենք» հասկացությունը, ամենայն հավանականությամբ, չէր կիրառվում ռազմական գործողություններ վարելու մեթոդի իմաստով: Այդ հասկացությանը, ըստ երևույթին, տրվում է ինչ-որ այլ իմաստ, որը ներառում է կամ չի ներառում «կիբեռզենք» կատեգորիան զինված հակամարտությունների իրավունքի իմաստով: Այստեղ հարկ է ընդգծել, որ այդ ժամանակահատվածում գիտական մակարդակով քննարկումների և դեբատների առարկա էր կիբեռզենքերի իրավաչափության հարցը, ինչով էլ հավանաբար պայմանավորված էր հիշյալ դրույթի ամրագրումը ՏԱ հայեցակարգով: Ակնհայտ է, սակայն, որ անկախ ՏԱ հայեցակարգի համատեքստում «տեղեկատվական զենք» եզրույթին տրված իմաստից, դրա մշակման, տարածման և կիրառման արգելքի նպատակի ամրագրումն ուներ անհարկի ինքնասահմանափակող բնույթ, քանի որ թե՛ տեղեկատվական տարբեր տեխնոլոգիաների կիրառումը պատերազմական ժամանակահատվածում՝ որպես հոգեբանական ներգործության միջոց (օրինակ, զինված հակամարտության ընթացքում հակառակորդի մասին սուտ տեղեկություններ տարածելը կամ, օրինակ, քարոզչությունը) և թե՛ հենց կիբեռզենքի ռազմական օգտագործումը ոչ միայն

սահմանումն ու տարբերակումը: Միևնույն ժամանակ, կիբեռանվտանգության ռազմավարության առկայությունը չի բացառում տեղեկատվական անվտանգության հայեցակարգի գոյությունը: Ընդհակառակը՝ այն լրացնում և ամբողջացնում է տեղեկատվական միջավայրում պետության անվտանգության ապահովման գործողությունները:

[163] ՆԿ-97, Հավելված, VIII.7:

[164] ՆԿ-97, Հավելված, VIII.10 կետ 3:

իրավաչափ է, այլև կարող է նպաստել առավելագույն ռազմական առավելությունների հասնելուն՝ ռեսուրսների նվազագույն ծախսերով:

Այսպիսով, ակնհայտ է, որ ՏԱ հայեցակարգն իրականում ուներ խոցելի կարգավորումներ, որոնց տրամագծորեն վերանայումը Հայաստանի Հանրապետության համար հրամայական էր՝ հաշվի առնելով Հայաստանի Հանրապետության և Արցախի Հանրապետության առջև ծառացած պետական պաշտպանության վտանգները: Մասնավորապես, կարևոր էր այսպես կոչված «տեղեկատվական զենք» եզրույթի հստակ սահմանումը և դրա վերաբերյալ պետական քաղաքականության հստակ ու ճշգրիտ տեսլական կազմելը, ինչպես նաև կիբեռզենքի մշակման ոլորտում հետազոտություններ իրականացնելու հնարավորության և անհրաժեշտության հարցի քննարկումը, որը կարող է կիրառվել միջազգային կամ ոչ միջազգային ռազմական հակամարտությունների շրջանակներում՝ Միջազգային հումանիտար իրավունքի հիմնական դրույթներին համապատասխան: Հատկանշական է, որ ՏԱ հայեցակարգում բացակայում են կիբեռտարածքում պաշտպանության և անվտանգության ապահովման վերաբերյալ դրույթները, և կիբեռտիրույթն առերևույթ անտեսված է:

ՏԱ հայեցակարգն ուժի մեջ մտնելուց հետո՝ 2010թ. փետրվարին հաստատվեց այս ոլորտում ՀՀ-ում էլեկտրոնային հասարակության ձևավորման հայեցակարգը ընդունելու մասին կառավարության որոշումը: Առանձնահատուկ հետաքրքրություն է ներկայացնում ՀՀ-ում էլեկտրոնային հասարակության ձևավորման մասին վերը նշված հայեցակարգի թիվ 4 Հավելվածը, որը կանոնակարգում է էլեկտրոնային անվտանգության ապահովման համար իրականացման ենթակա հատուկ գործողությունները, համապատասխան միջոցառումների իրականացման կոնկրետ ժամկետները, ինչպես նաև ակնկալվող արդյունքները:[165] Հիշյալ հավելվածի շրջանակներում հիմնական գործողություններից են, օրինակ, կիբեռանվտանգության հատուկ հանձնաժողովի ձևավորումը, «կիբեռանվտանգության» ընդհանուր սահմանների սահմանումը, նախնական աուդիտի իրականացումը և համապատասխան միջոցառումների իրականացման ժամանակ ՀՀ-ում տեղեկատվական անվտանգության վիճակի մասին ռիսկերի գնահատումը, այս ոլորտում օրենսդրության կատարելագործումը, կիբեռանվտանգության հատուկ ծրագրի մշակումը, պետական իշխանության

[165] ՀՀ կառավարության 2010 թ. փետրվարի 25–ի նիստի N7 արձանագրային որոշման Հավելված 4՝ էլեկտրոնային անվտանգություն (2010-2012 թթ.):

տարբեր մարմիններից, տեղական ինքնակառավարման մարմիններից և մասնավոր հատվածից կիբեռանվտանգության ապահովման ոլորտում հիմնական ներկայացուցիչների նշանակումը և վերապատրաստումը, կիբեռանվտանգության ապահովումը բոլոր կիրառական ուղղություններում, այդ թվում՝ հարկային, մաքսային, առողջապահության, պաշտպանության, էներգետիկայի, ոստիկանության և այլ, կիբեռհանցագործությունների կանխարգելմանն ուղղված նոր օրենսդրական կարգավորումների ընդունումը, պետական ծառայողների համար համապատասխան դասընթացների կազմակերպումը, հիմնական պետական կառույցներում (խորհրդարան, կառավարություն, նախագահի աշխատակազմ և այլ) անձնական տվյալների և տեղեկատվության անվտանգության ապահովումը, այս ոլորտում շարունակական հետազոտությունների իրականացումը և փորձի փոխանակման ապահովումը, Հայաստանի Հանրապետության ԱԱԾ-ի հետ սերտ համագործակցող կիբեռանվտանգության հատուկ խորհրդի ձևավորումը:[166] Հետաքրքիր է, որ ՏԱ հայեցակարգն ու ՀՀ-ում էլեկտրոնային հասարակության ձևավորման հայեցակարգը թեև գործնականում մշակվել են գրեթե զուգահեռ, սակայն ՏԱ հայեցակարգում առհասարակ չի հիշատակվում էլեկտրոնային հասարակության ձևավորումը նույնիսկ գաղափարական տեսանկյունից:

ՀՀ-ում էլեկտրոնային հասարակության ձևավորման հայեցակարգի իրականացումն ապահովելու նպատակով ՀՀ վարչապետի որոշմամբ 2011 թվականի հունվարին ստեղծվել էր Կիբեռանվտանգության պետական կոմիտե, որի կազմում ընդգրկվել էին Հայաստանի Հանրապետության Ազգային անվտանգության ծառայության, էկոնոմիկայի նախարարության, պաշտպանության նախարարության, տրանսպորտի և կապի նախարարության, ՀՀ գլխավոր դատախազության և ՀՀ կառավարությանն առընթեր ՀՀ ոստիկանության ներկայացուցիչները,[167] իսկ 2010 թվականի հունիսին ստեղծվել էր էլեկտրոնային կառավարման խորհուրդը:[168]

Ի պաշտոնե Էլեկտրոնային կառավարման հատուկ խորհրդի անդամներ են նշված հետևյալ անձինք՝ ՀՀ վարչապետը, ՀՀ փոխվարչապետը, ՀՀ էկոնոմիկայի

[166] ՀՀ կառավարության 2010 թ. փետրվարի 25–ի նիստի N7 արձանագրային որոշման (N 7) Հավելված 4, էջ 7-10:
[167] ՀՀ վարչապետի 2011 թվականի հունվարի 13-ի N 14 – Ա որոշում (N 14 – Ա), Հավելված 1՝ ներառյալ ՀՀ վարչապետի որոշումը (N 175 - Ա) N 14 – Ա որոշման մեջ փոփոխություն կատարելու և կիբեռանվտանգության պետական հանձնաժողովի անհատական կազմը հաստատելու մասին:
[168] ՀՀ վարչապետի 28 հունիսի 2010 թվականի N 475-Ն որոշումը ՀՀ էլեկտրոնային կառավարման խորհուրդ ստեղծելու, դրա կազմը և աշխատակարգը հաստատելու մասին (N 475 –Ն), ուժի մեջ է մտել 01.07.2010:

նախարարը, տրանսպորտի և կապի նախարարը, կրթության և գիտության նախարարը, ՀՀ ազգային անվտանգության ծառայության տնօրենը և ՀՀ ոստիկանապետը:[169] Էլեկտրոնային կառավարման խորհուրդը և կիբեռանվտանգության կոմիտեն համագործակցում և փոխգործակցում են. Մասնավորապես՝ կոմիտեի որոշումները ներկայացվում են խորհրդի հաստատմանը:[170] Իր հերթին, համաձայն վարչապետի որոշման, խորհրդի գործառույթները ներառում են կիբեռանվտանգության հայկական խորհուրդ ստեղծելու վերաբերյալ ՀՀ կառավարությանը առաջարկներ ներկայացնելը:[171]

Այս համատեքստում պետք է հաշվի առնել հետևյալ հիմնական գործոնները.

- ՀՀ էլեկտրոնային հասարակության ձևավորման հայեցակարգը, ինչպես և կիբեռանվտանգության կոմիտեի կազմը և էլեկտրոնային կառավարման խորհրդի կազմը հաստատվել են ՀՀ վարչապետի կողմից: Այսինքն՝ էլեկտրոնային հասարակության ձևավորման և կիբեռանվտանգության վերաբերյալ ՀՀ քաղաքականության ղեկավարումը ՀՀ վարչապետի գործառույթն էր:
- Հայեցակարգում «Կիբեռանվտանգություն» հասկացությունը ներառվել է էլեկտրոնային հասարակության ձևավորման համատեքստում: Հայեցակարգի իրականացումն ապահովելու նպատակով ստեղծված մարմինների (խորհուրդ և կոմիտե) գործառույթները ներառում են, ի թիվս այլոց, կիբեռանվտանգության ապահովման միջոցառումների իրականացումը: Այսինքն՝ կարգավորման առարկաներից մեկը պետության կիբեռանվտանգությունն է:
- Հայեցակարգը կարգավորում է որոշ ասպեկտներ, որոնք կարող են դիտարկվել որպես ազգային պաշտպանության ոլորտին առնչվող:[172] Ընդ որում, Կիբեռանվտանգության կոմիտեի անդամներից մեկը պաշտպանության նախարարության ներկայացուցիչ է (ՀՀ պաշտպանության նախարարի տեղակալ), սակայն պաշտպանության նախարարության ներկայացուցիչը ընդգրկված չէ էլեկտրոնային կառավարման համապատասխան խորհրդի կազմում: Միևնույն ժամանակ, հայեցակարգի համատեքստից կարելի է եզրակացնել, որ կիբեռանվտանգության ապահովում ասելով, ամենայն հավանականությամբ, հասկացվում է ՀՀ-ում կիբեռհանցագործությունների կանխարգելման

[169] *Ibid.*, Հավելված N 1:
[170] N 14 – Ա, supra n. 167, Հավելված 2, II:
[171] N 475 –Ն, supra n. 168, Հավելված N 2, II, 7:
[172] N 7, supra n. 166:

միջոցառումների իրականացումը, որոնք կարող են ուղղված լինել ինչպես ֆիզիկական անձանց, այնպես էլ պետության համակարգչային համակարգերի դեմ՝ դրանով իսկ վտանգ ներկայացնելով ազգային անվտանգության համար: Հայեցակարգի ձևակերպումներից, ինչպես նաև դրա իրականացման համար ստեղծված համապատասխան մարմինների կազմից երևում է, որ կիբեռանվտանգության ռազմական բաղադրիչներին տրվում է միայն երկրորդական նշանակություն, իսկ կիբեռհարձակումները չեն դիտարկվում որպես զինված հակամարտություններում Միջազգային հումանիտար իրավունքի իմաստով ռազմական գործողություններ իրականացնելու միջոց կամ մեթոդ: Հիշյալ որոշումները Հայկական կիբեռանվտանգության խորհուրդ ստեղծելու մասին կետ են նախատեսում, սակայն ազգային անվտանգության ծառայությունից պաշտոնապես ստացված տեղեկատվությունից, ինչպես նաև համապատասխան ակտերի ուսումնասիրությունից հետևում է, որ այդպիսի խորհուրդ դեռ չի ստեղծվել:

Ելնելով վերոգրյալից՝ հարկ է նշել, որ ՀՀ-ում կիբեռանվտանգության ոլորտում պետական առանձին ռազմավարական փաստաթղթերի մշակման, ինչպես նաև այս ոլորտում գործունեության իրականացման համար պատասխանատու ինստիտուցիոնալ կառուցակարգերի ստեղծման փաստն ինքնին առաջադեմ քայլ էր տվյալ ժամանակահատվածի համար: Այնուամենայնիվ, կիբեռտարածքի կարգավորմանը վերաբերող քննարկվող ռազմավարական փաստաթղթերը համապարփակ կերպով չէին արտացոլում ՀՀ ազգային շահերը և դրանք ակնհայտորեն անհրաժեշտ էր բարելավել՝ հաշվի առնելով զինված հակամարտությունների արդի մարտահրավերները՝ կիբեռտարածքի ռազմական օգտագործման պոտենցիալի, ռիսկերի և հնարավորությունների սահմանմամբ, կիբեռանվտանգության և պետական պաշտպանության միջև փոխկապակցվածության ընդգծմամբ, կիբեռպաշտպանության ոլորտում պաշտպանության նախարարության դերի մեծացմամբ, ռազմական կիբեռպաշտպանության ոլորտում մասնագիտացված կառույցի կամ ստորաբաժանման ստեղծման ծրագրմամբ, ինչպես նաև կիբեռզենքի մշակման ոլորտում հետազոտություններ իրականացնելու հնարավորության և անհրաժեշտության շեշտադրմամբ և որպես ռազմական քաղաքականության առաջնահերթություններից՝ կիբեռպաշտպանության, պաշտպանական կիբեռհարձակման և կիբեռզսպման կառուցակարգերի և ենթակառուցվածքների ձևավորմամբ: Այսպիսով, հաշվի առնելով ժամանակի ընթացքում ձևավորված միջազգային միտումները, տեղեկատվական անվտանգության ոլորտում պետական

քաղաքականությունն ուներ վերաիմաստավորման, իսկ ՏԱ հայեցակարգը՝ վերանայման անհրաժեշտություն: Այս ընկալումն առերևույթ առկա էր ՀՀ պաշտպանության սեկտորում, ինչի մասին է վկայում դեռևս 2014-2016թթ. ընթացքում ՀՀ ՊՆ Պաշտպանական ազգային հետազոտական համալսարանի Ազգային անվտանգության քաղաքականության և տեղեկատվական-հաղորդակցային տեխնոլոգիաների կենտրոնի կողմից մշակված և դոկտրինալ մակարդակում քննարկման ներկայացված ՀՀ կիբեռանվտանգության ազգային ռազմավարության նախագիծը:[173]

Կիբեռպաշտպանության ռազմավարական և ինստիտուցիոնալ* կարգավորումները *ՀՀ-ում 2018 թվականից առ այսօր

ՏԱ հայեցակարգը ուժը կորցրել է ՀՀ նախագահի 2017 թվականի նոյեմբերի 11-ի ՆԿ-97-Ն կարգադրությամբ, իսկ ՀՀ տեղեկատվական անվտանգության հայեցակարգի դրույթներով նախատեսված ծրագրերի իրականացումը համակարգող միջգերատեսչական հանձնաժողով ստեղծելու մասին ՀՀ նախագահի կարգադրությունն ուժը կորցրել է ՀՀ նախագահի 2018 թվականի ապրիլի 5-ին ՆԿ-49-Ն կարգադրությամբ: Տրամաբանորեն դրան պետք է հաջորդեր նոր ռազմավարության կամ ռազմավարությունների մշակումն ու ընդունումը, որով տարաբնույթ տեղեկատվական տեխնոլոգիաների կիրարկումը կսահմանվեր որպես երկրի տեղեկատվական քաղաքականության իրականացման իրավաչափ գործիք, կսահմանվեին կիբեռանվտանգության և կիբեռպաշտպանության իրականացման հիմնական կառուցակարգերը, իսկ կիբեռզենքերը կսահմանվեին որպես երկրի պաշտպանության համար օգտագործվող իրավաչափ միջոց և երկրի ռազմարդյունաբերության (սպառազինությունների) զարգացման իրավական եղանակ: Սա անհետաձգելի առանցքային խնդիր է՝ հատկապես հաշվի առնելով Հայաստանի Հանրապետության կառավարության բոլոր հնարավոր ոլորտների շարունակական թվայնացման ուղղությամբ ձեռնարկվող գործողությունները, մասնավորապես, ՀՀ կառավարության կողմից 2018 թվականին ընդունված «Խելացի քաղաքի» ստեղծման հայեցակարգի համատեքստում, որը ենթադրում է տարբեր տեխնոլոգիական լուծումներով հագեցած ենթակառուցվածքների ստեղծում՝

[173] Հայկական բանակ 1-2 (91-92), 2017 Հ. Ս. Քոթանջյան et.al, էջեր 61-72 (https://razmavaraget.files.wordpress.com/2017/07/armenian-army-n-1-2-2017.pdf): Հատկանշական է, որ ներկայացված փաստաթղթով սահմանվում էին նաև ոլորտին առնչվող հիմնական հասկացությունները:

առաջնային պլան մղելով համապատասխան ենթակառուցվածքների անվտանգության և պաշտպանության կազմակերպման խնդիրը:

ՏԱ հայեցակարգի 2017թ. հոկտեմբերին ուժը կորցրելուց հետո 2017 թվականին կառավարության կողմից մշակվել են ՀՀ կիբեռանվտանգության ռազմավարության, ինչպես նաև ՀՀ տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության ռազմավարության նախագծերը: Թվում էր, թե Հայաստանի Հանրապետության համար ռազմավարական նշանակություն ունեցող այս փաստաթղթերը պետք է պետության կողմից դիտվեին որպես առաջնահերթություն, լրամշակվեին ու կատարելագործվեին՝ միջազգային լավագույն փորձը հաշվի առնելով, վերջնականացվեին, վաղուց լինեին ընդունված և գտնվեին իրականացման փուլում: Սակայն իրողությունն այն է, որ 2017 թվականից առ այսօր Հայաստանի Հանրապետությունը չունի տեղեկատվական անվտանգության, ինչպես նաև կիբեռանվտանգության և ռազմական կիբեռպաշտպանության ոլորտներում որևէ ռազմավարական փաստաթուղթ:[174] Մինչդեռ ակնհայտ է, որ հնարավոր չէ ապահովել կիբեռանվտանգություն առանց ոլորտը համակարգող և կարգավորող հայեցակարգային, ռազմավարական և ընթացակարգային փաստաթղթերի: Եվ նման փաստաթղթերի մշակման և կյանքի կոչման համար անհրաժեշտ է խնդրի լրջության ընկալում, մասնագիտական ներուժի ակտիվացում և քաղաքական կամք:

Փոխարենը այսօր տեղեկատվական անվտանգությանն ու կիբեռանվտանգությանն անդրադարձող հիմնական դրույթները ամրագրված են 2020թ. հուլիսի 10-ի ՀՀ անվտանգության խորհրդի որոշմամբ ընդունված ՀՀ ազգային անվտանգության ռազմավարության 7-րդ բաժնի 7.9-7.16-րդ կետերով[175].

«7.9. Հայաստանի տեղեկատվական անվտանգության քաղաքականության հիմնական նպատակը անհատի, հասարակության և պետության շահերի հավասարակշռումն ու պաշտպանությունն է: Տեղեկատվական և կիբեռտիրույթներում մեր նպատակների իրագործման ճանապարհին մենք հիմնվում ենք մարդու իրավունքների ու ազատությունների և պետության ինքնիշխանության սկզբունքների վրա: Հայաստանը բաց, փոխգործունակ, հուսալի և անվտանգ համացանցի ջատագով է:

[174] Ավելին, ՀՀ օրենսդրության համապարփակ վերլուծությունը ցույց է տալիս, որ այսօր նույնիսկ տարրական անձնական տվյալների պաշտպանության մակարդակում օրենսդրորեն բացակայում են որևէ նվազագույն որակական տեխնիկական անվտանգության պահանջներ տեղեկատվությունը մշակողների նկատմամբ:

[175] ՀՀ ազգային անվտանգության ռազմավարություն, 10.07.2020, տես՝ https://www.mfa.am/filemanager/security%20and%20defense/AA-Razmavarutyun-Final.pdf:

7.10. Հայաստանի տեղեկատվական անվտանգությանը սպառնում են օտարերկրյա պետությունների, միջազգային ահաբեկչական կազմակերպությունների, հանցավոր խմբավորումների և անհատների կողմից Հայաստանի տարածքում գտնվող տեղեկատվական ռեսուրսների նկատմամբ կիբեռհարձակումները: Նոր և յուրահատուկ մարտահրավեր են մասնավոր կազմակերպությունների կողմից, ինչպես նաև օտար պետությունների ֆինանսավորմամբ ուղղորդվող կիբեռհարձակումները, որոնք թիրախավորում են Հայաստանի կենսական նշանակության տեղեկատվական ենթակառուցվածքները և դրանց կառավարման միջոցները:

7.11. Ժամանակակից աշխարհում ավելի սուր դրսևորումներ են ստանում տեղեկատվական պատերազմները, որոնք ներառում են քարոզչության, մանիպուլյացիաների, կեղծ լուրերի և ապատեղեկատվության գործիքակազմ և հաճախ թիրախավորում են ժողովրդավարական արժեքները: Այս համատեքստում մենք աշխատելու ենք հանրային իրազեկվածության և մեդիագրագիտության մակարդակի բարձրացման ուղղությամբ՝ նպատակ ունենալով հզորացնել տեղեկատվական պատերազմներին հակազդելու հասարակության և պետության կարողությունները:

7.12. Առաջնային մարտահրավերներից է տեղեկատվական և կիբեռանվտանգության ոլորտը կարգավորող համապարփակ պետական քաղաքականության անկատարությունը, կենսական նշանակության տեղեկատվական ենթակառուցվածքների պաշտպանությունն ապահովող օրենսդրության բացակայությունը, համակարգչային պատահարների արձագանքման կառույցների ինստիտուցիոնալ կարողությունների ոչ բավարար մակարդակը և կիբեռանվտանգության ոլորտը համակարգող կառույցի բացակայությունը:

7.13. Տեղեկատվական, տեխնոլոգիական և կիբեռանվտանգության ապահովման ոլորտում մենք աշխատում ենք ինստիտուտների և գործընթացների արդյունավետության մակարդակի բարձրացման և ենթակառուցվածքների զարգացման ուղղությամբ: Հայաստանը հետամուտ է տեղեկատվական, տեխնոլոգիական և կիբեռանվտանգության պետական քաղաքականության և ռազմավարությունների մշակմանը, ինչպես նաև ոլորտի կառավարման համապետական մեխանիզմների ներդրմանը: Մենք զարգացնելու ենք կենսական նշանակության տեղեկատվական ենթակառուցվածքներ ու թվային ծառայություններ մատուցողների և պետության միջև փոխհարաբերությունների նորմատիվ-իրավական դաշտը, ինչի արդյունքում կձևավորվեն նաև կիբեռանվտանգության ազգային կենտրոն և համակարգչային պատահարների արձագանքման խմբեր:

7.14. Տեխնոլոգիական անվտանգության տեսանկյունից Հայաստանը հետամուտ է կենսական կարևոր ոլորտներում և ենթակառուցվածքներում օգտագործվող տեխնոլոգիաներից և տեխնոլոգիական բաղադրիչներից առաջացող խոցելիությունների

չեզոքացմանը, օտար ծագման տեխնոլոգիաների ռիսկերի նվազեցմանը և ազգային տեխնոլոգիական հենքի զարգացմանը՝ այդ թվում նաև տեխնոլոգիաների մատակարարների հետ համագործակցության միջոցով:

7.15 Տեղեկատվական տիրույթում դիմակայունությունը բարձրացնելու համար մենք զարգացնելու ենք ազգային տեղեկատվական և կիբեռկարողությունները՝ ռիսկերի արդյունավետ կառավարման, որակավորված մասնագիտական ներուժի ձևավորման, միջազգային ստանդարտների տեղայնացված ներդրման, թվային գրագիտության մակարդակի բարձրացման միջոցով:

7.16. Ոլորտի դերակատարների բազմազանության, տեղեկատվական տիրույթում միջազգային սահմանների բացակայության և պետության, հասարակության ու մասնավոր հատվածների միջև կարողությունների բաժանվածության պայմաններում առանցքային է հանրային, մասնավոր և միջազգային հատվածների միջև համագործակցության մակարդակի բարձրացումը, ինչին էլ հետամուտ է լինելու պետությունը:»:

Վերոհիշյալ դրույթների վերլուծության արդյունքում կարելի է արձանագրել, որ.

1. ՀՀ ազգային անվտանգության ռազմավարությամբ արձանագրված են հանրահայտ ընդհանրական բնույթի ճշմարտություններ և վերացական նպատակներ: Տեղեկատվական, տեխնոլոգիական և կիբեռանվտանգության պետական քաղաքականության և ռազմավարությունների մշակումը, ինչպես նաև ոլորտի կառավարման համապատասխան մեխանիզմների ներդրումը նախատեսված են որպես այդ նպատակներից մեկը:

2. Ինչպես 2009 թվականի ՏԱ հայեցակարգում, այնպես էլ ՀՀ ազգային անվտանգության ռազմավարությամբ հստակեցված չէ «տեղեկատվական անվտանգություն» և «կիբեռանվտանգություն» հասկացությունների տարբերությունը, իսկ ռազմական կիբեռպաշտպանության կարողությունների ձևավորման անհրաժեշտությունն առհասարակ անտեսված է:

Ավելին, ՀՀ Ազգային անվտանգության ռազմավարությամբ «տեղեկատվական պատերազմ» ժարգոնի կիրառումը վկայում է այն մասին, որ ռազմավարության հեղինակները չեն հասկանում զինված հակամարտությունների համատեքստում կիբեռտարածքի օգտագործման իրական պոտենցիալը, ինչպես նաև առերևույթ չեն գիտակցում զինված հակամարտությունների ընթացքում տարբեր տեղեկատվական

տեխնոլոգիաների կիրառման իրավաչափությունն ու նշանակությունը որպես հոգեբանական ներազդման միջոց:

Մինչդեռ «տեղեկատվական անվտանգություն», «կիբեռանվտանգություն» և «կիբեռպաշտպանություն» հասկացությունների հստակ սահմանումը կհանդիսանար այն առաջին քայլը, որը կնպաստեր արդյունավետ կերպով դիտարկել ոլորտի խնդիրները, արտաքին և ներքին սպառնալիքները), մարտահրավերներն ու հնարավորությունները, ճշգրիտ գնահատել նշված հասկացություններով պայմանավորված պաշտպանական-անվտանգային համակարգերի իրավական, ինստիտուցիոնալ և տեխնիկական-տեխնոլոգիական տեսանկյուններից կայացվածության մակարդակը և ըստ այդմ մշակել համապատասխան քաղաքականություն, ռազմավարական դրույթներ և համապատասխան միջոցառումների ծրագրեր:

Կիբեռանվտանգության ապահովման կարևորությունն ամրագրված է նաև ՀՀ կառավարության 2021 թվականի փետրվարի 11-ի «Հայաստանի թվայնացման ռազմավարությանը, ռազմավարության միջոցառումների ծրագրին և արդյունքային ցուցանիշներին հավանություն տալու մասին» N 183-Լ որոշմամբ, որով, ինչպես և ՀՀ ազգային անվտանգության ռազմավարությամբ, նախատեսված են հանրահայտ ընդհանրական բնույթի ճշմարտություններ և վերացական նպատակներ, իսկ ռազմական կիբեռպաշտպանության խնդիրն ամբողջությամբ անտեսված է:[176]

2017 թվականին մշակված Կիբեռանվտանգության ռազմավարության նախագծի և 2017-2018 թվականներին մշակված ՀՀ տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության ռազմավարության նախագծի վերաբերյալ

Անդրադարձ կատարելով դեռևս 2017 թվականին մշակված և ավելի քան 4 տարիների ընթացքում այդպես էլ կառավարության ուշադրությանը չարժանացած, այդպես էլ չընդունված և չգործարկված Կիբեռանվտանգության ռազմավարության նախագծին, ինչպես նաև դեռևս 2017-2018 թվականներին մշակված և այդպես էլ թղթի վրա մնացած ՀՀ տեղեկատվական անվտանգության ապահովման և

[176] ՀՀ կառավարության 2021 թվականի փետրվարի 11-ի «Հայաստանի թվայնացման ռազմավարությանը, ռազմավարության միջոցառումների ծրագրին և արդյունքային ցուցանիշներին հավանություն տալու մասին» N 183-Լ որոշում, IV. 5-8, տես՝ https://www.arlis.am/DocumentView.aspx?docID=149957:

տեղեկատվական քաղաքականության ռազմավարության նախագծին, ապա դրանց վերլուծությունը վկայում է այն մասին, որ տեքստերը, չնայած դրանցում ներառված բազմաթիվ առաջադեմ կարգավորումների, այնուամենայնիվ կարիք ունեն բովանդակային մասնագիտական քննարկումների, լրամշակման և կատարելագործման՝ հաշվի առնելով կիբեռանվտանգության առկա արդի մարտահրավերներն ու կիբեռտարածքի ռազմական օգտագործման պոտենցիալն ու հնարավորությունները, ինչպես նաև ազգային անվտանգության և պետական պաշտպանության բնագավառներում Հայաստանի Հանրապետության առջև ծառացած խնդիրները:

Այսպես, մասնավորապես, Կիբեռանվտանգության ռազմավարության և դրանից բխող միջոցառումների ժամանակացույցի նախագծով.

- բացակայում է կիբեռանվտանգության, կիբեռպաշտպանության և տեղեկատվական անվտանգության հասկացությունների հստակ տարանջատումը՝ համապատասխանաբար բացակայում է ըստ ուղղությունների ձեռնարկվող միջոցառումների տարանջատումը,

- հիմնական շեշտադրումն իրականացվում է պետության կիբեռտարածքում ենթակառուցվածքների պաշտպանության վրա՝ առանց տարանջատելու պետության պաշտպանության ոլորտում առկա մարտահրավերները քաղաքացիական օբյեկտներին սպառնացող մարտահրավերներից, անտեսելով պետության պաշտպանական կիբեռհարձակումներ ձեռնարկելու և կիբեռզսպում իրականացնելու ուղղությունները, համապատասխանաբար՝ անտեսելով ՀՀ պաշտպանության նախարարության առաքելությունը երկրի կիբեռպաշտպանության կազմակերպման հարցում,

- հիմնականում ամրագրվում են վերացական նպատակներ և խնդիրներ, բացակայում են, մասնավորապես, ռազմական կիբեռպաշտպանության մասով ներկա իրավիճակի օբյեկտիվ նկարագիրը՝ թույլ և ուժեղ կողմերի, պետության կարողությունների գնահատականով, հստակ առաքելությունը և տեսլականը՝ հատկապես ռազմական կիբեռպաշտպանության բնագավառում, ինչպես նաև զինված հակամարտությունների ընթացքում տեղեկատվական տեխնոլոգիաների կիրարկման հարցով, յուրաքանչյուր ուղղության ռազմավարական նպատակները, ուղենիշները և խնդիրները, ռազմավարական ցուցանիշները և դրանց ստուգման

եղանակները, ձեռնարկվելիք գործողությունների *չափելի ծրագիրն ու* իրագործման համար անհրաժեշտ միջոցներն ու ռեսուրսները, ինչպես նաև ռազմավարության և գործողությունների ծրագրի իրականացման մշտադիտարկման և արդյունքների շարունակական գնահատման կառուցակարգերը:

Որպես ռազմավարության նախագծի կարևոր դրական կարգավորումներ՝ կարելի է առանձնացնել կիբեռանվտանգության կենտրոնի ստեղծման հանձնառությունը, ինչպես հանրային-մասնավոր համակործակցության և միջազգային համագործակցության խթանման անհրաժեշտության գիտակցումը:

Ինչ վերաբերում է 2017-2018 թվականներին մշակված ՀՀ տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության ռազմավարության նախագծին, ապա դրա հիմնական բովանդակությունից կարելի է հասկանալ, որ այն նպատակ չունի կարգավորելու, մասնավորապես, կիբեռտարածքի ռազմական օգտագործման հարցերը: Միևնույն ժամանակ, անհրաժեշտ է հիշյալ փաստաթղթով տարանջատել տեղեկատվական անվտանգության տիրույթը կիբեռանվտանգությունից և կիբեռպաշտպանությունից՝ չանտեսելով նաև այս ոլորտների փոխկապակցվածությունն ու համատեղ միջոցառումներ իրականացնելու անհրաժեշտությունը: Հարկ է նաև ընդգծել, որ ՀՀ տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության ռազմավարության նախագծով ևս համապարփակ ներկայացված չէ պետության տեսլականն ու քաղաքականությունը տեղեկատվական տիրույթում բովանդակություն ձևավորելու, տարբեր տեղեկատվական միջոցառումներ նախաձեռնելու և ՀՀ շահերին դեմ նախաձեռնված տեղեկատվական միջոցառումներին ակտիվ հակազդելու վերաբերյալ: Նախագծով որդեգրված է ինստիտուցիոնալ ապակենտրոնացվածության մոտեցումը, ինչը կարող է արդյունավետ լինել միայն միջոցառումների և գործողությունների պատասխանատուների հստակ սահմանմամբ ու միասնական համակարգող մարմնի հստակեցմամբ: Կարևոր է նաև նշել, որ ինչպես և Կիբեռանվտանգության ռազմավարության և դրանից բխող միջոցառումների ծրագրի նախագծում, այս ռազմավարական փաստաթղթում ևս բացակայում են յուրաքանչյուր ուղղության ռազմավարական նպատակները, ուղենիշները և խնդիրները, ռազմավարական ցուցանիշները և դրանց ստուգման եղանակները, ձեռնարկվելիք գործողությունների *չափելի ծրագիրն ու* իրագործման համար անհրաժեշտ միջոցներն ու ռեսուրսները, ինչպես նաև ռազմավարության և

գործողությունների ծրագրի իրականացման մշտադիտարկման և արդյունքների շարունակական գնահատման կառուցակարգերը:

Այս համատեքստում կարևորում ենք ընդգծել հետևյալը.

1. Ցանկացած ռազմավարություն պետք է ունենա որոշակի կառուցվածք և որոշակի խորությամբ բովանդակություն:

2. Պետական կառավարման մարմինների կողմից տեղեկատվական անվտանգության, կիբեռանվտանգության և ռազմական կիբեռպաշտպանության ոլորտների զարգացման, քաղաքականության ձևավորման և ռազմավարությունների մշակման ու իրականացման հարցում պետական կառավարման մարմինների դրսևորած պասիվ կեցվածքը կամ անգործությունն անթույլատրելի են՝ հաշվի առնելով Հայաստանի Հանրապետության առջև ծառացած մի շարք անվտանգային և պաշտպանական խնդիրները:

3. Տեղեկատվական անվտանգության, ինչպես նաև կիբեռանվտանգության և կիբեռպաշտպանության ոլորտներում պետական քաղաքականության մշակումն ու համապատասխան ռազմավարությունների հնարավորինս օպերատիվ կերպով ընդունումը պետք է պետության կողմից դիտարկվեն որպես առաջնահերթություն: Միևնույն ժամանակ, համապատասխան փաստաթղթերը մշակելիս կամ առկա նախագծերը լրամշակելիս և կատարելագործելիս անհրաժեշտ է հաշվի առնել հետևյալ սկզբունքներն ու ուղղությունները.

3.1. Պետության կողմից մշակվող ռազմավարությունը, որպեսզի այն լինի արդյունավետ և իրագործելի, պետք է առնվազն ներառի՝ 1) ներկա իրավիճակի օբյեկտիվ նկարագիրը, թույլ և ուժեղ կողմերը, առկա մարտահրավերները, կարողությունների օբյեկտիվ գնահատականը, 2) առաքելությունը և տեսլականը, 3) առաքելությունից և տեսլականից բխող ընդհանուր նպատակը կամ հիմնական ուղությունները (սկզբունքները), 4) յուրաքանչյուր ուղղության ռազմավարական նպատակները, 5) յուրաքանչյուր նպատակի ռազմավարական ուղենիշները և խնդիրները, ինչպես նաև չափելիությունն ապահովող՝ 6) ռազմավարական ցուցանիշը, 7) ցուցանիշի ստուգման աղբյուրը, 8) միջոցառումները, 9) գործողությունների *չափելի ծրագիր*, 10) անհրաժեշտ միջոցներ (ռեսուրսներ), հստակ պատասխանատուներ և ժամկետներ, 11) ռազմավարության և գործողությունների

ծրագրի իրականացման մշտադիտարկման և արդյունքների շարունակական գնահատման կառուցակարգեր:

3.2. Ռազմավարություններով պետք է հստակ սահմանված լինի ռազմավարության իրականացման նկատմամբ վերահսկողական կառուցակարգ՝ պետական ներկայացուցչական ամենաբարձր մակարդակով:

3.3. Ռազմավարություններով պետք է հստակեցված լինեն կարգավորման առարկան և դրա իրավական բովանդակությունը, տեղեկատվական անվտանգություն, կիբեռանվտանգություն և ռազմական կիբեռպաշտպանություն եզրույթները պետք է հստակ տարանջատվեն՝ յուրաքանչյուրի համար նախատեսելով համապատասխան վերաբերելի կարգավորումներ:

3.4. Տեղեկատվական անվտանգության ռազմավարությունը պետք է պարունակի դրույթներ ոչ միայն ՀՀ դեմ իրականացվող գործողություններին «հակազդելու» տրամաբանությամբ, այլ նաև պետք է նախատեսի պետության քաղաքականությունը՝ միջազգային իրավունքին համապատասխան անվտանգային և պաշտպանական խնդիրների լուծմանն ուղղված տեղեկատվական տեխնոլոգիաների ուսումնասիրության և գործարկման մասով:

3.5. Տեղեկատվական անվտանգության ռազմավարությամբ հատուկ անդրադարձ պետք է իրականացվի արհեստական բանականության արդյունքում տեղեկատվական դաշտում ծագող մարտահրավերներին արդյունավետ արձագանքելուն ուղղված գործողությունների ծրագրին, ինչպես նաև արհեստական բանականության կիրարկմամբ ոլորտի զարգացման հնարավորությունների բացահայտմանն ուղղված նպատակների, խնդիրների, միջոցառումների ու գործողությունների ձևակերպմանը:

3.6. Կիբեռանվտանգության ռազմավարությամբ առանձին անդրադարձ պետք է իրականացվի կիբեռանտվանգության և պետության պաշտպանության միջև կապին՝ հաշվի առնելով կիբեռտարածության մեջ քաղաքացիական և ռազմական ենթակառուցվածքների փոխկապակցվածությունը:

3.7. Կիբեռտարածքի կարգավորմանն ուղղված ռազմավարական փաստաթղթերը մշակելիս անհրաժեշտ է նկատի ունենալ այն իրողությունը, որ 21-րդ դարում պատերազմ վարելու կիբեռմիջոցները կարող են կիրառվել սովորական

զենքերի հետ զուգահեռ: Հետևապես պետության կողմից պետք է կարևորվի կիբեռզենքերի ստեղծման և դրանք պետության պաշտպանության համար օգտագործելու միտումը: Ռազմական կիբեռպաշտպանության ոլորտում պետության քաղաքականությունը պետք է տեղ գտնի կա՛մ առանձին ռազմավարության տեսքով,կա՛մ կիբեռանվտանգության ռազմավարության առանձին բաժնի տեսքով:

3.8. Տեղեկատվական անվտանգության, կիբեռանվտանգության և կիբեռպաշտպանության քաղաքականությունը, ներառյալ՝ համապատասխան կենտրոնների ստեղծումն ու գործարկումը, պետք է իրականացվի պետություն-մասնավոր հատված համագործակցության մոդելով՝ ներգրավելով համաշխարհային լավագույն ներուժն ու օգտագործելով լավագույն միջազգային փորձը:

ԱՄՓՈՓՈՒՄ

Կիբեռտարածքն արդեն վաղուց դիտարկվում է որպես պետությունների կողմից պատերազմ վարելու սովորական հարթակ, ինչպես ցամաքային, օդային և ջրային տարածքները: Ուստի, ՀՀ պարտականությունն է ձևավորել տվյալ հարցի վերաբերյալ պետության տեսլականն ու մշակել դրա իրականացմանն ուղղված ռազմավարությունն ու գործողությունների ծրագիրը՝ որպես պետության պաշտպանության կարևոր բաղկացուցիչ մաս: Եվ չնայած միջազգային համագործակցության արդյունքում ՀՀ-ում իրականացվող կիբեռպաշտպանության վերաբերյալ որոշակի գործնական միջոցառումներին,[177] ՀՀ-ում ռազմական կիբեռպաշտպանության վերաբերյալ տեսլականի, քաղաքականության և ռազմավարական փաստաթղթերի բացակայությունը վտանգավոր իրողություն է՝ պետական պաշտպանության արդյունավետ կազմակերպման համատեքստում: Խնդրի արդիականության և հրատապության մասին են վկայում նաև ՀՀ կիբեռանվտանգության և կիբեռպաշտպանության ապահովման մասով միջազգային գնահատականները: Այսպես, 2020 թվականի համաշխարհային կիբեռանվտանգության ինդեքսի հրապարակած տվյալների համաձայն՝ Հայաստանի գնահատականը 50,47 է և Հայաստանն իննսուներորդն է կիբեռանվտանգության հուսալիության տեսանկյունից:[178]

[177] ՀՀ տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության ռազմավարության նախագիծ, II.7.3:
[178] Global Cybersecurity Index 2020, supra n. 74.

Ավելին, տարածաշրջանի երկրներից (Ռուսաստան, Ղազախստան, Ադրբեջան, Ուզբեկստան, Բելառուս, Հայաստան, Ղրղզստան, Տաջիկստան, Թուրքմենստան) Հայաստանի ցուցանիշը զգալիորեն ավելի ցածր է, քան Ռուսաստանի, Ղազախստանի, Ադրբեջանի և Ուզբեկստանի ցուցանիշները, և 0,10-ով ավելի ցածր է, քան Բելառուսի ցուցանիշը: Այսինքն՝ Հայաստանից ավելի ցածր ցուցանիշներ են միայն Ղրղզստանում (49,64), Տաջիկստանում (17,1) և Թուրքմենստանում (տվյալները բացակայում են):

Իսկ ազգային կիբեռանվտանգության ինդեքսով 2020 թվականի դրությամբ Հայաստանն այլ պետությունների շարքում 90-րդն է՝ ունենալով նվազագույն զրոյական ցուցանիշ կիբեռանվտանգության քաղաքականության մշակման առումով (0%), նվազագույն զրոյական ցուցանիշ կիբեռտարածքում վտանգների վերլուծության տեսանկյունից (0%), նվազագույն զրոյական ցուցանիշ կիբեռտարածքում ճգնաժամի կառավարման տեսանկյունից (0%), նվազագույն զրոյական ցուցանիշ կենսական ենթակառուցվածքների և թվային ծառայությունների պաշտպանության տեսանկյունից (0%) և նվազագույն զրոյական ցուցանիշ ռազմական ոլորտում կիբեռօպերացիաների կազմակերպման կարողությունների տեսանկյունից (0%):[179]

[179] NCSI for Armenia, at: https://ncsi.ega.ee/country/am/.