ОБОРОНА И БЕЗОПАСНОСТЬ

Կիբերտարածությունում ռազմական հակամարտությունների կարգավորման խնդիրները

Հակոբյան Էրիկ Ա.
հայցորդ, Միջազգային հարաբերությունների ֆակուլտետ,
Երևանի պետական համալսարան (Երևան, ՀՀ)
https://orcid.org/0009-0009-7491-0051
erik.hakobyan.2020@gmail.com

ՀՏԴ՝ 355.4; **EDN:** DCTTNY
DOI: 10.58587/18292437-2026.5-49
Հանգուցաբառեր և բառակապակցություններ՝ կիբերտարածություն, կիբերպատերազմի մասնակիցներ, նորարարություն, բազմակողմ ռեժիմ, էլեկտրամագնիսական սպեկտր, միջազգային պայմանագիր:

Вопросы регулирования военных конфликтов в киберпространстве

Акопян Эрик А.
Аспирант, Факультет международных отношений
Ереванский государственный университет (Ереван, РА)

Аннотация. В статье утверждается, что, несмотря на стремительное наращивание национальных киберарсеналов, в настоящее время отсутствует международный консенсус относительно применения норм права вооруженных конфликтов к кибервойне, которая, как правило, рассматривается как разновидность «нерегулярных боевых действий». Данная неопределенность обусловлена как быстрым распространением методов ведения кибервойны, так и отсутствием прецедентов международного регулирования враждебных вторжений в киберпространство.
В статье рассматриваются ключевые принципы права вооруженных конфликтов, которые могли бы лечь в основу обсуждения будущих положений потенциального договора или резолюции, касающихся киберпространства.
Ключевые слова и словосочетания: киберпространство, субъекты кибервойны, инновации, многосторонний режим, электромагнитный спектр, международный договор

The Issues of Regulating Military Conflicts in Cyberspace

Hakobyan Erik A.
PhD candidate, Faculty of International Relations,
Yerevan State University (Yerevan, RA)

Abstract. This article argues that despite the rapid accumulation of national cyber arsenals, there is currently no international consensus regarding the application of the "law of armed conflict" to cyber warfare—which is generally considered a form of "irregular warfare." This ambiguity stems from both the rapid proliferation of cyber warfare methods and the lack of precedents for the international regulation of hostile incursions into cyberspace.
The article examines key principles of the law of armed conflict that could serve as a basis for discussing future provisions of a potential treaty or resolution concerning cyberspace.
Keywords & phrases: cyberspace, cyber warfare actors, innovation, multilateral regime, electromagnetic spectrum, international treaty

Սույն աշխատանքում «կիբերպատերազմ» տերմինն օգտագործվում է ամենալայն իմաստով և ներառում է կիբերտարածության միջոցով այլ երկրների կամ ազդեցիկ ոչ պետական դերակատարների կողմից վնաս պատճառելու հետ կապված տարբեր գործողություններ: Տերմինը կարող է նշանակել տեղեկատվական և հաղորդակցական համակարգերի, կարևոր ենթակառուցվածքների և օբյեկտների պաշտպանություն, զինատեսակների համակարգերի կամ ռազմական հրամանատարական կենտրոնների վրա հարձակումներից պաշտպանություն, ինչպես նաև հակառակորդի դեմ համարժեք հարձակողական գործողությունների իրականացում: Իսկ էլեկտրամագնիսական սպեկտրը, որը ևս պատկանում է այս շարքին, անշուշտ, դիմակայության նոր ոլորտ չէ, սակայն կործանարար նորարարությունները և մարդկանց՝ տեխնիկայից աճող կախվածությունը առցանց թիրախները դարձնում են ավելի ու ավելի գրավիչ այն պետությունների համար, որոնք ձգտում են նվազագույն ծախսերով հասնել առավելագույն

ազդեցության: Սա հատկապես արդիական է փոքր պետությունների համար, որոնք ցանկանում են XXI դարի մարտադաշտում ստանալ ասիմետրիկ առավելություն: Թեև պատերազմի վարման կիբեռնետիկական հնարքներն ու մեթոդները դեռ միայն ձևավորվում են, կիբերզենքի և «կիբերռազմիկների» նոր սերունդը խոստանում է փոխակերպել XXI դարի պատերազմները: Եթե հաջորդ պատերազմն իսկապես վարվելու է կիբերտարածությունում, ապա ի՞նչ կարող է անել միջազգային հանրությունը՝ այդ ոլորտը կարգավորելու կամ դրա նկատմամբ վերահսկողություն իրականացնելու համար: Հաշվի առնելով կիբերպատերազմների և միջազգային հարաբերությունների միջև աճող փոխկախվածությունը՝ սույն աշխատանքում փորձ կարվի հիմնավորել բազմակողմ ռեժիմի ներդրման անհրաժեշտությունը, որը հնարավորություն կարող է տալ գլոբալ մակարդակով կարգավորել կիբերպատերազմները: Կիբերպատերազմներ վարելու համար մշակվում են եզակի, երբեմն բազմամակարդակ միջոցներ, որոնք կարող են լինել ինչպես պաշտպանական, այնպես էլ հարձակողական: Հենց բազմամակարդակ պաշտպանության համակարգի ստեղծման անհրաժեշտությունը պայմանավորված է նրանով, որ բոլոր հեռանկարային կիբերհամակարգերի փոխկապակցումը նախատեսվում է իրականացնել օգտատերերի համար՝ անկախ նրանց մակարդակից, միասնական գլոբալ հաղորդակցական ցանցի միջոցներով: Սա ուղղված է այն նպատակին, որ մշակվող միջոցները (ցանցային ծածկագրման սարքեր, ծրագրային և տեխնիկական միջոցների համալիր) պետք է ապահովեն տեղեկատվական ռեսուրսներին հասանելիության օրինականության ստուգումը, օգտատերերի նույնականացումը, սպառողների և անձնակազմի կողմից կատարվող բոլոր գործողությունների գրանցումը՝ դրանց օպերատիվ և հետագա վերլուծության հնարավորությամբ՝ պահպանելով գաղտնիության անհրաժեշտ մակարդակը:

Հակառակորդի տեղեկատվական ռեսուրսների կազմում ներթափանցման և դրանց վրա ազդեցության եղանակների համաձայն՝ ծրագրային-տեխնիկական ներգործության հարձակողական միջոցները բաժանվում են հետևյալ դասերի.

- «տրամաբանական ռումբ»՝ թաքնված կառավարման ծրագիր, որը որոշակի ազդանշանի կամ նախապես սահմանված ժամանակի դեպքում ակտիվանում է՝ ոչնչացնելով կամ աղավաղելով տեղեկատվությունը, արգելափակելով կառավարվող տեղեկատվական ռեսուրսի որոշ կարևոր հատվածների հասանելիությունը կամ ապակազմակերպելով տեխնիկական միջոցների աշխատանքը: Զորքերի և սպառազինության ավտոմատացված կառավարման համակարգերում նման միջամտությունը կարող է արմատապես ազդել մարտի կամ գործողության ընթացքի և ելքի վրա [**1**].

- «ծրագրային վիրուս»՝ մասնագիտացված ծրագրային արտադրանք, որն ունակ է վերարտադրել տրամաբանական ռումբերը և դրանք հեռահար կերպով ներդնել հակառակորդի տեղեկատվական ցանցերում, ինքնուրույն բազմապատկվել, կցվել ծրագրերին և փոխանցվել ցանցի միջոցով [**2**].

- «տրոյական ձի»՝ ծրագիր, որի ներդրումը հնարավորություն է տալիս գաղտնի, չարտոնված մուտք գործել հակառակորդի տեղեկատվական զանգված՝ հետախուզական տեղեկատվություն ստանալու նպատակով [**3**].

- տեքստային ծրագրերի չեզոքացուցիչ, որն ապահովում է ծրագրային ապահովման բնական և արհեստական թերությունների պահպանումը.

- դիտավորյալ ստեղծված և սովորական օգտագործողից թաքցված՝ համակարգ մուտք գործելու ինտերֆեյսներ, որոնք մշակողների կողմից ներդրվում են ծրագրային ապահովման մեջ շահադիտական կամ դիվերսիոն-քայքայիչ նպատակներով.

- փոքրաչափ սարքեր, որոնք ունակ են գերներացնել բարձր հզորության էլեկտրամագնիսական իմպուլսներ՝ ապահովելով ռադիոէլեկտրոնային սարքավորումների շարքից դուրս գալը:

Առավելագույն հնարավոր վնաս հասցնելու տեսանկյունից ծրագրային-տեխնիկական ներգործության միջոցների կիրառման առաջնահերթ օբյեկտներ կարող են համարվել հրթիռային հարձակման նախազգուշացման և տիեզերական տարածության վերահսկման համակարգերի տեղեկատվական տարրերը, բարձրագույն օղակի կառավարման կետերը, ինչպես նաև դրանք սպասարկող հաշվողական կենտրոններն ու կապի հանգույցները: Խաղաղ ժամանակ նմանատիպ ազդեցություն կարող է իրականացվել նաև պետության համար կարևոր օբյեկտների նկատմամբ, ինչպիսիք են բանկային համակարգը, օդային երթևեկության կառավարման համակարգը, ինչպես նաև հակառակորդ պետության բնակչության վրա հոգեբանական ազդեցություն գործադրելու իրողությունը, հատկապես սահմանամերձ շրջաններում, ռադիո- և հեռուստահաղորդումների միջոցներով:

Ծրագրային-տեխնիկական ներգործության միջոցների բնորոշ հատկանիշներից կարելի է նշել գործողության արմատականությունը և կեղծ ընտրողականությունը, համընդհանուր կիրառելիությունը, գաղտնիությունը, անսպասելիությունը, տնտեսապես շահավետ լինելը, բազ-

մատարբերակությունը և տարածաժամանակային մանևրի ազատությունը:

Թեև աշխարհը դեռևս չի վարել համապարփակ կիբերպատերազմներ, կիբերարտադրանքների փորձագետներն ու ռազմական ռազմավարները ակնկալում են, որ իրական միջպետական կիբերպատերազմ արդեն առաջիկա տարիներին կարող է ծավալվել [**4**]: Միջազգային անվտանգության տեսանկյունից առանձնահատուկ մտահոգություն է առաջացնում այս ոլորտում աճող սպառնալիքի պայմաններում կարգավորման և վերահսկողության չափազանց թույլ համակարգը: Քանի որ մոլորակի բնակչության համար կենսական նշանակություն ունեցող գործառույթների ավելի ու ավելի մեծ մասն իրականացվում է կիբերտարածության միջոցով, լայնածավալ կիբերհարձակման սոցիալ-տնտեսական հետևանքները կարող են կաթվածահար անել ժամանակակից պետությունը, որի գործունեության բոլոր ոլորտները ներթափանցված են ցանցային համակարգերով: ԱՄՆ Ռազմավարական հրամանատարության (USSTRATCOM)[1] գեներալ Քևին Չիլթոնը, որի տեսակետը կիսում են բազմաթիվ ռազմական ղեկավարներ, կարծում է, որ տեղեկատվական առումով զարգացած տնտեսություն ունեցող երկրի նկատմամբ լուրջ կիբերհարձակումը կարող է հանգեցնել սովորական սպառազինության լայնածավալ պատասխան հարվածի, իսկ առանձին դեպքերում՝ նույնիսկ միջուկային միջոցների կիրառման [**5**]: Նրա խոսքերով՝ ազգային ռազմավարները «*չեն բացառում կիբերտարածությունում ռազմական գործողություններին արձագանքելու որևէ տարբերակ*»:

Կիբերտարածությունում «բոլորը բոլորի դեմ պատերազմները» կանխելուն ձգտելով՝ միջազգային հանրությունը բախվում է հսկայական կառուցվածքային խնդիրների: Քառորդ դարից էլ պակաս ժամանակահատվածում «կիբերտարածություն» տերմինը, որը ներմուծել է գիտաֆանտաստիկայի ժանրի գրող Ուիլյամ Գիբսոնը, վիրտուալ աշխարհի հասկացությունից վերածվել է արագ զարգացող ցանցային հասարակության թվային աշխարհի: USSTRATCOM-ը միավորում է զինված ուժերի բոլոր տեսակները, ինչպես նաև ներառում է Պաշտպանության նախարարության կապալառու կազմակերպություններին և քաղաքացիական անձանց: Տեղեկատվական և հաղորդակցական տեխնոլոգիաների սրընթաց առաջընթացը գրեթե 2 միլիարդ «թվային» քաղաքացիների կապել է կիբերտարածության անտեսանելի միջավայրում[2]:

Բարդ սխեմաների և ծրագրային ապահովման այս թվային ոլորտը վերածվեց ռազմական գործողությունների նոր թատերաբեմի և մարտադաշտի, երբ Վիետնամի պատերազմից հետո ԱՄՆ-ի ռազմական ռազմավարության էվոլյուցիայի ուսումնասիրությունների բնույթը փոխվեց այլ ուղղությամբ:

Ի պատասխան XX դարի սրընթաց տեխնոլոգիական առաջընթացի՝ ռազմականվերլուծաբաններն ու ֆուտուրոլոգները, գիտակցելով պատերազմների վարման ավանդական ռազմավարության հնացածությունն ու ոչ ադեկվատ լինելը, քննարկում էին, թե ինչպես է տեղեկատվական գալիք դարը փոխելու պատերազմների վարման եղանակները: Դրանով զբաղվում էին ոչ միայն Միացյալ Նահանգները, այլև մյուս երկրները, որոնք, սակայն, չէին կարող համեմատվել տեղեկատվական պատերազմների հայեցակարգերի մշակման և զարգացման ուղղությամբ ամերիկյան ներդրումների մասշտաբների հետ: «Տեղեկատվական պատերազմների» ոլորտում նման պլանավորման մեծ մասը իրականացվում էր մի շարք նոր զինատեսակների համակարգերի և ծրագրերի մշակման հիմնավորման նպատակով, այդ թվում՝ ժամանակակից ինտերնետի նախորդի՝ ARPANET-ի (Advanced Research Projects Agency Network)՝ համակարգչային ցանցի, որը ստեղծվել էր ԱՄՆ Պաշտպանության նախարարության Առաջադեմ հետազոտական նախագծերի գործակալության կողմից:

Երբ տեղեկատվական համակարգերը դարձան ռազմական գործողությունների կարևոր մաս, մշակվեց տեղեկատվական պատերազմի (ՏՊ) ամերիկյան նոր դոկտրինը: Դրանով ռազմական գործողությունների ֆիզիկական թատերաբեմերին (ցամաք, ծով և օդ) ավելացան էլեկտրամագնիսական սպեկտրը և տեղեկատվական տարածությունը: ՏՊ-ի նպատակն էր տեղեկատվական միջոցներն օգտագործել որպես ռազմավարական զենք հակառակորդին մոլորեցնելու և նրան չմտածված գործողությունների դրդելու համար: Թեև կիբերտարածության գոյության առաջին տասնամյակներին տեղեկատվական և հաշվողական տեխնոլոգիաները պարզունակ էին՝ համեմատած ներկայում առկա տեխնոլոգիաների հետ, ԱՄՆ-ի ռազմական ղեկավարությունը չէր կասկածում, որ XXI դարում տեղեկատվական պատերազմները դուրս կմղեն մնացած պատերազմաձևերը: ԱՄՆ-ի համար 1990-ականների վերջին ռազմական գործում

[1] «Կիբեր» տերմինը ներմուծել է Նորբերտ Վիները իր «Կիբեռնետիկա, կամ կառավարում և հաղորդակցություն կենդանու և մեքենայի մեջ» գրքում (Cambridge, MA: MIT Press, 1948): «Կիբերտարածություն» տերմինը Գիբսոնն առաջին անգամ օգտագործել է իր վաղ շրջանի պատմվածքներից մեկում, այնուհետև՝ իր հայտնի «Նեյրոմանսեր» վեպում (New York: Ace Books, 1984):

[2] 2009 թվականի սեպտեմբերի 30-ի դրությամբ ամբողջ աշխարհում ինտերնետ օգտագործողների ընդհանուր թիվը գնահատվում էր 1,733,993,741 մարդ [**7**]:

տեղի ունեցած հեղափոխությունը նշանակում էր փոփոխություններ երեք ոլորտներում՝ տեղեկատվական գործողություններ, սպառազինության համակարգեր և տիեզերք: Դրանց Մայքլ Շմիթը ավելացնում է ռազմական գործի հեղափոխության չորրորդ սերունդը՝ քաղաքացիական գործունեության ռազմականացումը [**8**, էջեր 394-400]: Դրանով նա նկատի ունի քաղաքացիական անձնակազմի և քաղաքացիական ենթակառուցվածքների ինտեգրումը XXI դարի ռազմական գործողությունների թատերաբեմին:

2000 թվականից սկսած՝ պետությունների կողմից ֆինանսավորվող կիբերնետիկական ներթափանցումների գրանցված փորձերը տատանվել են՝ կառավարական վեբկայքերի կոտրումից մինչև կենսական նշանակություն ունեցող ենթակառուցվածքների վրա հարձակումներ: Ըստ ԿՀՎ-ի հաղորդումների՝ 2007 թվականին կիբերհարձակումների են ենթարկվել մի շարք տարածաշրջաններում գործող մի քանի հանրային էլեկտրամատակարարման ցանցեր՝ ինչպես ԱՄՆ-ի տարածքում, այնպես էլ նրա սահմաններից դուրս: Կոմունալ ծառայությունների ղեկավարները խիստ դժկամությամբ են խոսում այդ վտանգի մասին: 2009 թվականի վերջին ԱՄՆ-ի պաշտոնաթող ծովակալ Մայքլ ՄաքՔոնելը, որը տարբեր ժամանակներում ղեկավարել է ԿՀՎ-ն, Ռազմական հետախուզության գործակալությունը և Ազգային անվտանգության գործակալությունը, հայտարարել է, որ ԱՄՆ-ն ունի այնպիսի հակառակորդներ, որոնք ի վիճակի են անջատել ԱՄՆ-ի էներգահամակարգի հիմնական հատվածները [**9**]: Համակարգը կոտրելով՝ առաջադեմ հաքերը կարող է ստանալ նույն հասանելիությունն ու լիազորությունները, ինչ համակարգի ադմինիստրատորը [**10**]: 2005 թվականից Բրազիլիայի քաղաքներում գրանցվում են հարձակումներ տվյալների հավաքագրման և դիսպետչերական կառավարման SKADA ծրագրային-ապարատային համալիրի վրա[3]: Ջոն Մալդերը՝ ԱՄՆ էներգետիկայի նախարարությանը կից Sandia Laboratories-ի անվտանգության մասնագետը, պատմել է, թե ինչպես է Sandia-ն[4], ստանալով էներգետիկ և ջրամատակարարող ընկերությունների համաձայնությունը, հայտնաբերում նրանց համակարգերի խոցելիությունները՝ փորձելով կոտրել այդ համակարգերը և այլ կարևոր թիրախներ, որպեսզի մշակի համապատասխան պաշտպանական միջոցներ [**11**]:

2007 թվականին Էստոնիայի ցանցերի և 2008 թվականին Վրաստանի պետական համակարգերի դեմ լայնորեն լուսաբանված հարձակումները, ինչպես ենթադրվում էր, իրականացվել էին ռուսաստանցի հայրենասիրական տրամադրվածություն ունեցող հաքերների կամ Ռուսաստանի պաշտոնական գործակալների կողմից [**12**]: ՆԱՏՕ-ն Էստոնիայի ցանցի անջատմանը արձագանքեց Հյուսիսատլանտյան խորհրդի արտակարգ նիստի հրավիրմամբ, իսկ 2008 թվականին Բուխարեստում կայացած գագաթնաժողովում դաշինքը հայտարարեց իր առաջին կիբերպաշտպանության քաղաքականության մասին: Սա առաջին դեպքն էր, երբ միջազգային ռազմական կազմակերպությունը կիբերանվտանգությունը ճանաչեց որպես հավաքական պաշտպանության բաղադրիչ: ՆԱՏՕ-ն հայտարարում է, որ անդամ պետության դեմ զանգվածային կիբերհարձակման դեպքում դաշինքի կիբերանվտանգության նոր քաղաքականությունը հնարավորություն է տալիս արդյունավետ և համարժեք արձագանքելու [**13**, էջեր 51, 52]:

Ինչպես ահաբեկչության դեմ պայքարը, այնպես էլ կիբերանվտանգությունը միաժամանակ և՛ ներքին իրավապահ մարմինների, և՛ զինված ուժերի գործն է, հատկապես երբ հաճախ հնարավոր չէ մեկը մյուսից տարանջատել: Վերոնշյալ օրինակները հստակ ցույց են տալիս, որ ինտերնետի աշխատանքին միջամտությունն այժմ կարող է շարքից դուրս բերել կենսական նշանակություն ունեցող ենթակառուցվածքները կամ ռազմական ցանցերը:

Կիբերանվտանգության դիրքերի ամրապնդմանը զուգահեռ ազգային անվտանգության համակարգում բազմաթիվ երկրների կառավարություններ «ռազմական գործողությունները» հակառակորդի առցանց գոտի տեղափոխելու համար պատրաստ են ընդլայնել իրենց ունեցած հնարավորությունները: ԱՄՆ ռազմաօդային ուժերի հետախուզական վարչության դատավոր-փաստաբան, գնդապետ Չարլզ Ուիլյամսոնը հայտարարում է, որ աշխարհը հրաժարվել է իրական աշխարհում ամրոցի մտածելակերպից, և պետք է դուրս գալ դրա սահմաններից ու անցնել կիբերտարածություն, քանի որ յուրաքանչյուր պետություն բախվում է իր ռազմական և քաղաքացիական կիբերտարածություններում անընդհատ աճող սպառնալիքների: Նա ցանկանում է, որպեսզի հուսալի զսպում ապահովելու համար ԱՄՆ-ը հնարավորություն ունենա կիբերտարածությունում իրականացնելու «զորգային ռմբակոծություններ»: Այդ նպատակով,

[3] SCADA-ն միկրոպրոցեսորային կառավարմամբ հանրային ենթակառուցվածքների համաշխարհային ստանդարտ է, որը լայնորեն կիրառվում է ձեռնարկություններում, պետական էներգետիկ և տրանսպորտային ցանցերում: Տեղեկատվությունը կարող է հավաքագրվել տարբեր վայրերում և փոխանցվել կենտրոնական համակարգչին:

[4] Լինելով պետական պայմանագրային կազմակերպություն՝ Sandia-ն իրականացնում է հետազոտություններ և տալիս փորձագիտական եզրակացություններ միջուկային զենքի, պաշտպանության համակարգերի և ներքին անվտանգության, ինչպես նաև էներգետիկ ռեսուրսների անվտանգության հետ կապված հարցերի վերաբերյալ:

նրա կարծիքով, անհրաժեշտ է ստեղծել «բոտնետ»՝ բոտերով վարակված համակարգիչների («զոմբիների») ցանց, որը կկարողանա թիրախային համակարգիչներին ուղարկել այնքան հսկայական քանակությամբ տրաֆիկ, որ դրանք կկորցնեն միմյանց հետ կապ պահպանելու ունակությունը և անօգուտ կդառնան հակառակորդների համար: Այլ կերպ ասած՝ նրա պնդմամբ, եկել է ժամանակը հրաժարվելու անցյալի հակամարտությունների ռազմավարությունից և հզոր ու ճկուն զսպման համակարգ ստեղծելու համար օգտագործելու թվային հնարավորություններն ու փորձը, որը հնարավորություն կտա հասնել հակառակորդին «ամրոցի» սահմաններից շատ հեռու և հարված հասցնել նրան, քանի դեռ դրա հնարավորությունը կա [**14**];

ԱՄՆ-ը առաջինն սկսեց զբաղվել կիբերպատերազմների և հրամանատարական նախաձեռնությունների քաղաքականությամբ՝ ստանձնելով առաջատար դիրք այս ոլորտներում, սակայն 2007 թվականից մի շարք պետություններ նույնպես սկսեցին ամրապնդել իրենց կիբերպաշտպանությունը՝ փորձելով այդ գործընթացի վրա չհրավիրել միջազգային հանրության ուշադրությունը: Այս նախաձեռնությունները ներառում են ամեն ինչ՝ սկսած ապագա կիբերռազմիկների հավաքագրումից մինչև լիարժեք կիբերհրամանատարությունների ստեղծում: Որպես կանոն, կիբերտարածության համար ռազմական կառավարման համակարգի ստեղծումը նշանակում է, որ պետությունը ձգտում է կիբերհարվածներ հասցնելու հնարավորություններ ձեռք բերել:

Եզրակացություն և խնդիրների լուծման առաջարկություններ

Հոդվածի ուսումնասիրությունը ցույց է տալիս, որ կիբերտարածության ռազմականացումը և կիբերհարձակումների աճող վտանգը առաջացնում են մի շարք փոխկապակցված խնդիրներ՝ պետական և ռազմական համակարգերի խոցելիություն, կենսական ենթակառուցվածքների պաշտպանության դժվարություններ, մասնագետների պակաս, կիբերհարձակումների աղբյուրի նույնականացման բարդություն և կիբերպատերազմի նկատմամբ միջազգային իրավական կարգավորման անբավարարություն:

Այս խնդիրների լուծման համար առաջին հերթին անհրաժեշտ է **ուժեղացնել ազգային կիբերպաշտպանության համակարգերը**: Մշտական մոնիթորինգի, անվտանգության պարբերական աուդիտների և արագ արձագանքման կենտրոնների միջոցով հնարավոր է հարձակումները հայտնաբերել ավելի վաղ և նվազեցնել դրանց հետևանքները: Սա հատկապես կարևոր է ռազմական և պետական համակարգերի համար, որոնց խափանումը կարող է անմիջականորեն ազդել երկրի անվտանգության և կառավարման արդյունավետության վրա:

Առանձնահատուկ ուշադրություն պետք է դարձնել **կենսական նշանակություն ունեցող ենթակառուցվածքների պաշտպանությանը**: Էներգետիկ, ֆինանսական, տրանսպորտային և կապի համակարգերի խափանումը կարող է ունենալ ոչ միայն տեխնիկական, այլև տնտեսական և սոցիալական լուրջ հետևանքներ: Այդ պատճառով անհրաժեշտ է պարբերաբար գնահատել դրանց խոցելիությունները, իրականացնել անվտանգության ու դիմակայունության թեստեր և ապահովել պահուստային համակարգերի առկայությունը:

Մյուս կարևոր ուղղությունը **կիբերանվտանգության մասնագետների պատրաստումն ու տեխնիկական կարողությունների զարգացումն** է: Կիբերսպառնալիքների արագ փոփոխվող բնույթը պահանջում է ոչ միայն ժամանակակից տեխնոլոգիաներ, այլև համապատասխան մասնագիտական գիտելիքներ: Կրթական և վերապատրաստման ծրագրերի զարգացումը, ինչպես նաև պետական և մասնավոր հատվածների համագործակցությունը կարող են նպաստել մասնագետների պակասի նվազեցմանը և ազգային կիբերունակությունների ամրապնդմանը:

Կիբերհարձակումների միջազգային բնույթը նաև պահանջում է **պետությունների միջև ավելի սերտ համագործակցություն**: Հարձակումների աղբյուրի բացահայտման և պատասխանատու կողմի նույնականացման դժվարությունը կարող է նվազեցվել թվային փորձաքննության, տեխնիկական հետաքննության և օպերատիվ տեղեկատվության փոխանակման մեխանիզմների զարգացման միջոցով: Սա կարևոր է ինչպես հարձակումներին արդյունավետ արձագանքելու, այնպես էլ ապագա միջադեպերը կանխելու համար:

Վերջապես, անհրաժեշտ է **կատարելագործել կիբերպատերազմի միջազգային իրավական կարգավորումը**: Կիբերուժի կիրառման աճը, առանց հստակ միջազգային կանոնների, մեծացնում է սխալ գնահատումների և հակամարտությունների սրման վտանգը: Պետությունների պատասխանատվության, կիբերհարձակումների թույլատրելի սահմանների և միջազգային արձագանքի վերաբերյալ ավելի հստակ նորմերի ձևավորումը կարող է նպաստել կիբերտարածությունում կանխատեսելիության և կայունության բարձրացմանը:

Այսպիսով, կիբերանվտանգության ապահովումը պահանջում է տեխնիկական, կազմակերպչական, մասնագիտական և իրավական միջոցների համակցում: Միայն նման համալիր

մոտեցումը կարող է նվազեցնել կիբերսպառնալիքների ազդեցությունը և բարձրացնել պետությունների դիմակայունությունը կիբերտարածությունում:

Օգտագործված գրականության ցանկ

1. Information Warfare: New Roles for Information Systems in Military Operations, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/crawford.pdf
2. 4 Threats and Vulnerabilities: A Brief Overview, https://nist-sp-800-12-r1.bsafes.com/docs/4-threats-and-vulnerabilities-a-brief-overview/
3. Trojan horse, https://csrc.nist.gov/glossary/term/Trojan_Horse
4. Nathan Hodge's speech on May 13 2009. URL: http://www.wired.com/danger-room/2009/05/ general-we-just-might-nuke-those-cyber-attackers/
5. Kevin Chilton's speech at the Cyberspace Symposium, held on April 7, 2009, in Omaha. URL: http://www.stratcom.mil/speeches/23/2009
6. Jeff Schogol's on May 8 2009. URL: http://www.stripes.com/article.asp?section=i04&article=62555
7. 'Internet usage statistics: the internet big picture', Internet World Stats on Sept. 30 2009. URL: http://www.internet-worldstats.com/stats.htm
8. **Schmitt Michael** "Bellum Americanum", The law of armed conflict into the next millennium (Newport: Naval War College, 1998)
9. **United States Cyber-Conseruences Unit** "Urgency of this cyber-security work", URL: http://www.usccu.us/#The_Urgency_of_This_Cyber-Security_Work
10. **Gorman Siobhain** "Electricity grid in US penetrated by spies", Wall Street Journal, 8 April 2009.
11. "Cyber-war: Sabotaging the system", 60 Minutes CBS broadcast, 8 Nov. 2009. URL: http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml
12. **Markoff John and Kramer Andrew** "US and Russia differ on a treaty for cyber", 27 June 2009. URL: http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=1
13. **Hughes Rex** "NATO and global cyber defense." The Bucharest Conference Papers, 2008.
14. **Williamson Charles** "Carpet bombing in cyberspace." Armed Forces Journal, 2010. http://www.armedforcesjournal.com/2008/05/3375884

Сдана / Հանձնվել է՝ 14.07.2026
Рецензирована / Գրախոսվել է՝ 21.07.2026
Принята / Ընդունվել է՝ 28.07.2026