ERMƏNİSTAN KİBERMƏKANINDA QHT-LƏRİN ROLU

Elnur KƏLBİZADƏ*

Xülasə: Kibertəhlükəslizlik müasir dövrdə dövlətlərin milli təhlükəsizliyinin vacib tərkib hissələrindən biridir. Hər bir dövlət mövcud olduğu fiziki məkan kimi, kiberməkana da nəzarət etmək, onu öz maraqları və mənafeləri naminə yönləndirmək uğrunda mübarizə aparır. Lakin kiberməkanla bağlı siyasətin dövlətlər tərəfindən sadəcə öz imkanları hesabına reallaşdırmaq çətindir. Bu baxımdan bir çox ölkələr kiberməkanda QHT-lərin gücündən də istifadə edirlər. Məqalədə başlıca məqsəd Ermənistanın kiberməkanında qeyri-hökumət təşkilatlarının rolunu və funksiyalarını tədqiq etməkdən ibarətdir. Mövzunun öyrənilməsi Ermənistan cəmiyyətinin siyasi strukturunda QHT-lərin rolunun öyrənilməsi baxımından nəzəri, milli kibertəhlükəsizlik baxımından isə praktiki aktuallığa malikdir.
Tədqiqat siyasi yönümlüdür və daha çox siyasi elmin metodlarından istifadə etməklə Ermənistan kiberməkanı ilə bağlı məsələlərinin qiymətləndirilməsini nəzərdə tutur.
Açar sözlər: *Kiberməkan, Kibertəhlükəsizlik, QHT, Ermənistan, Cənubi Qafqaz*

The Role of Ngos in Armenian Cyberspace

Abstract: Cybersecurity is a crucial component of national security for states in the contemporary era. Just as each state contends for control over its physical territory, it also engages in efforts to monitor and direct the cyberspace in line with its own interests and objectives. However, for states, the implementation of cyber policies solely through their own capacities poses challenges. Hence, many countries leverage the power of non-state actors in the cyberspace. The primary objective of this article is to investigate the role and functions of non-governmental organizations (NGOs) in Armenia's cyberspace. The study of this topic is theoretically significant for understanding the role of NGOs in the political structure of Armenian society and practically relevant for national cybersecurity. The research is politically oriented and aims to evaluate issues related to Armenia's cyberspace primarily using political science methodologies.
Keywords: *Cyberspace, Cybersecurity, NGOs, Armenia, South Caucasus*

Giriş

Müasir dünyada dövlətlərin gücü onların təkcə fiziki məkanda deyil, həm də kiberməkanda olan gücü ilə müəyyənləşir. Kibersiyasətin həyata keçirilməsi dövlət siyasətinin vacib istiqamətlərindən biri hesab edilir. Kibertəhlükəsizlik milli təhlükəsizliyin ən vacib komponentlərindən sayılır. Lakin xarakter etibarilə kiberməkan elə bir mühitdir ki, orada təhlükəsizliyin təmin edilməsi dövlət institutlarının təkbaşına yerinə yetirə biləcəkləri vəzifə deyildir. Məhz bu baxımdan bir çox ölkələrdə mərkəzi dövlət aparatı və institutları digər sahələrin idarə edilməsi ilə yanaşı, kibersiyasətin həyata keçirilməsində də bəzi funksiyaları qeyri-hökumət təşkilatlarına ötürür, onlardan kibersiyasətin həyata keçirilməsi, kibertəhlükəsizliyin təmin edilməsi vasitəsi kimi istifadə edirlər.

Üçüncü dünya ölkələrində kibersiyasətin həyata keçirilməsinin alətlərindən biri kimi qeyri-hökumət təşkilatlarından istifadə edilməsi həm də dövlətlərin və rəsmi hakimiyyət orqanlarının bir çox məsələlərlə bağlı məsuliyyətdən yayınma vasitəsi hesab edilir. Bu cəhətdən uzun illər ərzində qonşularına qarşı ərazi iddiaları ilə çıxış edən, təkcə müharibə meydanında deyil, virtual məkanda da təcavüzkar mövqe tutmuş Ermənistanda kibersiyasətin həyata keçirilməsində qeyri-hökumət təşkilatlarının (QHT) rolunun öyrənilməsi ciddi siyasi və nəzəri əhəmiyyətə malikdir. Tədqiqatın başlıca məqsədi Ermənistanda hazırki şəraitdə kibersiyasətin həyata keçirilməsində QHT-lərin rolunun müəyyən edilməsindən, onların kibertəhlükəsizlik problemlərinin aradan qaldırılmasında hansı rolu oynamasının qiymətləndirilməsindən ibarətdir.

1. QHT-Lərin Kibertəhlükəsizlikdə Oynaya Biləcəyi Rol Nədən İbarətdir?

QHT-lər bir çox ölkələrdə kibertəhlükəsizlikdə həlledici rol oynayır. Hökumət agentlikləri və özəl sektor qurumları tez-tez kibertəhlükəsizlik problemlərinin həllində liderlik

* Dosent, AMEA Qafqazşünaslıq İnstitutunun Ermənişünaslıq Şöbəsinin Müdiri, Bakı Avrasiya Universitetinin Humanitar Fənlər və Regionşünaslıq Kafedrasının Dosenti, e-mail: kelbizadeh@gmail.com

etsələr də, QHT-lərin də bu sahədə rolu özünəməxsusdur. QHT-lərin ölkələrin kibertəhlükəsizliyinin təmin edilməsində və kibersiyasətlərinin həyata keçirilməsində spesifik rolundan bəhs edərkən bir neçə məqamı xüsusi vurğulamaq olar. İlk növbədə QHT-lər həm milli, həm də beynəlxalq səviyyədə daha yaxşı kibertəhlükəsizlik siyasəti və qaydalarının yaradılması təşəbbüsləri ilə çıxış etmək, bu istiqamətdə dövlətlərin siyasətinə təsir etmək imkanlarına malikdirlər. Bir sıra inkişaf etmiş ölkələrdə onlar kibertəhlükəsizliklə bağlı ən yaxşı təcrübələri, məlumatların qorunmasını və məxfilik hüquqlarını təşviq edən qanunvericiliyə təkan verərək siyasətçilər və geniş ictimaiyyət arasında kibertəhlükəsizlik problemləri haqqında məlumatlılığı artırırlar.

Digər tərəfdən QHT-lər kibertəhlükəsizlik təhdidləri və onların azaldılması yolları haqqında fərdləri, biznes və dövlət qurumlarını maarifləndirmək üçün seminarlar, təlim sessiyaları və ictimai məlumatlandırma kampaniyaları təşkil edirlər. Bura təhlükəsiz internet istifadəsi, parol idarəçiliyi, fişinq cəhdlərinin tanınması, şəxsi və təşkilati məlumatların təhlükəsizliyi kimi mövzular daxildir.

QHT-lər kibertəhlükəsizlik mütəxəssisləri, hüquq-mühafizə orqanlarının işçiləri və hökumət rəsmiləri üçün təlim və bacarıqların artırılması proqramları təmin edirlər. Bu proqramlar kritik infrastrukturun qorunması və kiber insidentlərə cavab verən şəxslərin bacarıq və biliklərini təkmilləşdirməklə ölkənin ümumi kibertəhlükəsizlik mövqeyini gücləndirməyə kömək edir. Bundan əlavə QHT-lər kibertəhlükəsizlik təhdidləri və ayrı-ayrı ölkələrə xas olan tendensiyalar üzrə araşdırma aparır, həmçinin regional və qlobal miqyasda digər təşkilatlarla məlumat mübadiləsi təşəbbüslərində iştirak edirlər. QHT-lər kibertəhlükəsizlik risklərini effektiv şəkildə idarə etmək üçün resursları və ya təcrübəsi olmayan təşkilatlara texniki yardım və dəstək təklif edir, kibertəhlükəsizlik qiymətləndirmələrinin aparılmasını, təhlükəsizlik tədbirlərinin həyata keçirilməsinə dair təlimatın verilməsini və ya kiberhücum zamanı insidentlərə cavab xidmətlərini təklif edirlər.

İnkişaf etmiş cəmiyyətlərdə QHT-lər kibertəhlükəsizlik barədə məlumatlılığı təşviq etmək və kibertəhlükəsizlik şüurunu inkişaf etdirmək üçün məktəblər, universitetlər və yerli təşkilatlar da daxil olmaqla yerli icmalarla iş aparırlar.

Bəzi dövlətlər üçün isə QHT-lərin kibertəhlükəsizlik məsələlərinin həllində iştiraka cəlbi məsuliyyətdən yayınma vasitəsidir. Bu mənada müasir dünyada kibermüharibə, kiberhücum və kibermüdafiə anlayışları ilə yanaşı kiberterrorçuluq anlayışı da fərqləndirilir. Ölkənin kibermüdafiəni təmin etdiyi, kibermüharibə apardığı yoxsa kiberterrorizmlə məşğul olduğu isə konkret praktikada qiymətləndirilə bilər. Kibersiyasət və təhlüksəziliklə bağlı ölkələrin qanunvericiliklərində bəyan etdikləri yazılı prinsiplər isə çox zaman elə yazı olaraq qalır. Belə ölkələrdən biri məhz Ermənistandır.

2. Ermənistanda Kibercinayətkarlığa Bağlı Hüquqi Baza və Onun İcrası Mexanizmləri

Avropa Şurasının Octopus Community kibercinayətkarlıq və elektron sübutlar üzrə məlumat mübadiləsi və əməkdaşlıq platformasının Ermənistanla bağlı açıqladığı məlumatlarda qeyd edilir ki, bu ölkədə hazırda kibercinayətkarlıqla bağlı xüsusi strategiya və ya fəaliyyət planı yoxdur. Lakin tədqiqatlar göstərir ki, Ermənistanda informasiya təhlükəsizliyinə dövlət yanaşması 2009-cu ildə formalaşmağa başlayıb. Buna səbəb həmin dövrdə bir sıra dövlət saytlarına növbəti haker hücumu olub. Bu hadisədən bir müddət sonra, 2009-cu ildə iyunun 26-da Ermənistan Prezidenti Ermənistan Respublikasının informasiya təhlükəsizliyi konsepsiyasını təsdiqləmişdi. Həmin ilin sonunda işçi qrup yaradılmışdı ki, oraya daxil olan mütəxəssislər bu məsələdə dövlət siyasətinin əsaslarını işləyib hazırlamalı və onların həyata keçirilməsi üçün prioritet tədbirləri müəyyən etməli idilər. 2022-ci ildən etibarən kibercinayətkarlıq siyasətini ehtiva edən hərtərəfli Kibertəhlükəsizlik Strategiyasının hazırlanması üçün bir neçə Hökumət qurumunun birgə səyi ilə işə başlanılmışdı. Lakin 2024-cü ilin fevralında açıqlanan məlumatlardan aydın olur ki, Ermənistan hökuməti

kibertəhlükəsizlik üçün institusional çərçivələrin formalaşdırılmasına yönəlmiş strateji tədbirləri həyata keçirə bilməyib.

Ermənistan Respublikasının Milli Təhlükəsizlik Xidməti kibertəhlükəsizlik siyasətinə və hökumət saytlarının və şəbəkələrinin qorunmasına cavabdehdir. Bundan əlavə, 2009-cu ildə İnformasiya Təhlükəsizliyi Strategiyasının konsepsiyası işlənib hazırlanmışdır ki, bu da həyata keçirilməli olan müəyyən fəaliyyətləri əks etdirir. Ermənistanın Rəqəmsallaşma Strategiyası 2021-ci ilin fevralında qəbul edilib və kibertəhlükəsizlik fəaliyyətləri və kibertəhlükəsizlik və məlumatların mühafizəsi sahəsində qanunlarla bağlı müəyyən tədbirləri ehtiva edir.

Lakin Ermənistanda qüvvədə olan cinayət-prosessual məcəlləsində kibercinaytkarlıqla bağlı birbaşa maddələr yer almamışdır. Ölkənin 2007-ci ildə qəbul edilmiş "Əməliyyat-axtarış fəaliyyəti haqqında" Qanunun 26-cı maddəsinə istinad edərək dövlət hakimiyyəti orqanları ölkə vətəndaşlarının kompyuterlərinin izlənilməsi və onların məlumatlarının toplanılmasını da həyata keçirə bilir (Cybercrime in Armenia, 2024).

Ermənistanda kibertəhlükəsizliyin təmin olunmasında bir sıra dövlət qurumları əsas rol oynayırlar.

Ermənistan Respublikası Polisinin Cinayətkarlıqla Mübarizə Baş İdarəsi nəzdində Yüksək Texnologiyalar üzrə Cinayətkarlıqla Mübarizə Şöbəsi ölkə miqyasında kibercinayətkarlıqla mübarizəni təşkil edən mərkəzləşdirilmiş bölmədir. Şöbə kibercinayətkarlıqla bağlı işlərə ilkin mərhələdə (İstintaq Komitəsi tərəfindən rəsmi araşdırma başlamazdan əvvəl) baxan və yerli bölmələrə dəstək verən əsas polis bölməsidir. Bu şöbədə 2024-cü ilə olan məlumatlara görə 8 nəfər əməkdaş çalışır. Qurumun ixtisaslaşmış yerli bölmələri yoxdur. Zəruri hallarda Mütəşəkkil Cinayətkarlıqla Mübarizə İdarəsinin əlavə resurslarından istifadə olunur. Şöbə haking (məlumatların oğurlanması və sındırılması), strateji əhəmiyyətli kiber-infrastruktura hücumlar, məlumatların qeyri-qanuni ələ keçirilməsi və onlara müdaxilə kimi kompüter sistemlərinə qarşı törədilən cinayətləri araşdırmaq səlahiyyətinə malikdir. Şöbə, həmçinin internet fırıldaqçılıq, texnologiyalardan uşaqlara qarşı sui-istifadə, əqli mülkiyyət hüquqpozmaları ilə bağlı cinayətlərlə məşğul olmaq səlahiyyətlərinə malikdir. Onun fəaliyyət istiqamətlərindən biri də texnoloji irqçilik və texnoloji ksenofobiya kimi cinayətlərlə mübarizədir. Lakin Ermənistanmərkəzli kibermühitə diqqət yetirmək kifayətdir ki, bu qurumun ümumiyyətlə bu istiqamətdə fəaliyyət göstərmədiyi aydın olsun. Bir tərəfdən texnoloji irqçiliyə və ksenofobiyaya qarşı mübarizə apardığını elan edən Ermənistanın hökumət qurumları digər tərəfdən qonşu ölkələrə, o cümlədən Azərbaycan Respublikasına, Türkiyə Cümhuriyyətinə, Rusiya Federasiyasına, Gürcüstana qarşı kiberiqçiliyi və kiberksenofobiyanı dəstəkləyirlər.

Bu sahədə fəaliyyət göstərən digər bir qurum Ermənistan Respublikasının İstintaq Komitəsidir. 2011-ci ildə cinayət-prosessual islahatlardan sonra Ermənistanda cinayət işlərinin 95%-i İstintaq Komitəsi tərəfindən araşdırılır. Komitədə kibercinayətlərlə bağlı işlərlə məşğul olan 6 müstəntiq vardır. Onların funksiyası kibercinayətlərlə bağlı istintaq proseslərinə rəhbərlik etmək və daha sonra onları prokurora təqdim etməkdir.

CERT-AM Ermənistan hökumətinin nəzarətində olan Kompüter sistemləri ilə bağlı Fövqəladə Hallara Cavab Mərkəzidir. Bu qurum Ermənistanda dövlət orqanları ilə bağlı baş vermiş kiberhadisələr haqqında məlumatları toplayır, saxlayır və təhlil edir. Qurum qeydə alınmış kompüter insidentlərinin təhqiqatını aparır və bu barədə dövlət orqanları üçün hesabatlar hazırlayır. Kibermüdaxilələrin qarşısını almaq üçün tədbirlər görür. Kiber insidentlərin araşdırılması zamanı CERT-AM Ermənistan xüsusi xidmət və hüquq-mühafizə orqanları ilə fəal əməkdaşlıq edir (Կենտրոնի մասին - Համակարգչային Միջադեպերի արձագանքման պետական կենտրոն , 2024).

2019-2020-ci illəri təhlil edən bir araşdırmaya görə nə qədər paradoksal olsa da Ermənistanda vətəndaş cəmiyyəti institutlarına qarşı kiberhücumların başlıca qaynağı rolunda

Ermənistan hökumətinin özü, keçmiş rejimə (S. Sarkisyan rejiminə) bağlı qüvvələr çıxış etmişdir (Digital security incidents against the Armenian Civil Society in 2019 – 2020, 2023, p. 4).

2020-ci il martın 16-da Hökumət Ermənistan vətəndaşları üçün bir sıra məhdudiyyətlər tətbiq etməklə fövqəladə vəziyyət elan etmişdi. Qərar parlamentin Paşinyanın "Mənim addımım" alyansının üzvlərinin üstünlük təşkil etdiyi növbədənkənar iclasında təsdiqlənmişdi. "Həyəcanverici təşviqatın" qarşısının alınması zərurətini əsas gətirərək hökumət qərara almışdı ki, COVID-19 ilə bağlı vəziyyətin bəzi spesifik aspektləri ilə bağlı sosial mediada yayılan xəbərlər və yazılar rəsmi hesabatları əks etdirməli, bu məlumatlardan kənara çıxmamalıdır.

Hazırki dünya tamamilə fərqli bir məkandır. Artıq dövlətlər bir-birlərinə qarşı hibrid müharibələr apardıqlarını gizlətmirlər. Bunun vasitələrindən biri də kibermüharibələrdir. Birmənalı şəkildə demək mümkündür ki, real döyüş meydanında olduğu kimi, virtual məkanda da son üç ildə Azərbaycan Ermənistan üzərində əzici üstünlük əldə etmişdir. Uzun illər işğal siyasəti yürütmüş Ermənistan özünün kibertəhlükəsizliyini də təmin etmək iqtidarında deyildir. 2019-cu ilə aid statistik məlumatlarda qeyd edilirdi ki, Ermənistanın kiberhücumlara məruz qalan ölkələr arasında 14-cü yeri tuturdu. Ermənistanın özündə də etiraf edirdilər ki, bu həmin sektorun koordinasiya olunmaması ilə bağlıdır (Դեհերյանը & Գեւորգյանը, 2019). 2024-cü ilin ilk aylarına olan məlumatlarda qeyd edilir ki, Qlobal Kibertəhlükəsizlik İndeksinə (GCI) əsasən Ermənistan kibertəhlükəsizlik səviyyəsinə görə 193 ölkə arasında 90-cı yerdə qərarlaşmışdır. Müqayisə üçün qeyd edək ki, həmin dövrdə kibertəhlükəsizlik indeksinə görə Türkiyə 11-ci, Azərbaycan 40-cı, İran 54-cü, Gürcüstan isə 55-ci olmuşdur. MDB ölkələri arasında yalnız Qırğızıstan, Tacikistan və Türkmənistan Ermənistandan aşağı göstəricilərə malikdir (Մելքոնյան, 2024).

Başqa bir məqam isə ondan ibarətdir ki, bir çox hallarda Ermənistana qarşı kiberhücumlar təşkil edən ən müxtəlif qruplar müəyyən simvollardan istifadə edərək bunu Azərbaycanın və ya Türkiyənin hücumları kimi göstərməyə çalışırlar. Hətta bir çox Erməni mütəxəssisləri də etiraf edirlər ki, bu cür hücumlar üçüncü ölkələrdən təşkil edilir, belə olan halda Azərbaycan və Türkiyəyə aid simvollar sadəcə kiberhücumçular üçün örtük rolunu oynayır.

Ermənistanın kiberməkanının təhlükəsiz olmadığını göstərən bir neçə fakta diqqət yetirək.

2023-cü ilin noyabrında Ermənistan mediasında yayılan bir məlumatda göstərilirdi ki, Ermənistan məktəblərində istifadə olunan dərsliklərin elektron versiyalarının yerləşdiyi saytlarda yerləşdirilən QR kodlar skan edilərkən avtomatik olaraq Türkiyə bayrağı yerləşdirilmiş sayta keçid olurdu (Հակոբյան, Հայկական դասագրքերի QR կոդերը տարել են թուրքական դրոշով կայք, ըստ ԿԳՄՄՆ պաշտոնյայի՝ ոչինչ 100%-ով պաշտպանված չի լինել չի կարող, 2023). Həmin saytın Ermənistanın Elm, Təhsil, Mədəniyyət və İdman Nazirliyinin nəzarətində olmasına və elektron dərsliklərin QR kodlarının xüsusi hazırlanmasına baxmayaraq onların kiberhücumlara davam gətirməməsi bir daha Ermənistan kiberməkanının hansı vəziyyətdə olduğunu göstərir.

Həmin dövrdə Ermənistan təhlükəsizlik ekspertlərindən biri Ermənistanın demək olar ki, əksər dövlət, hökumət nümayəndələrinin, ictimai xadimlərinin hesablarının casus proqramları ilə yoluxdurulduğuna dair məlumat açıqlamışdı. Həmin insanların bir çoxu casus proqramına cəmiyyət tərəfindən qınanılacaq saytlara daxil olaraq yoxumuşdular. Məhz bu səbəbdən də mütəxəssislərə müraciət edərkən də məsələnin gizli qalmasına çalışırdılar. İT eksperti S.Martirosyan demişdi: *"Həmin insanlar bizimlə gizli şəkildə əlaqə saxlayırlar. Onlar bunun ictimailəşməsini istəmirlər. Belə şəxslərin sayı yüzlərlədir. Bizimlə əlaqə saxlayanlar rəsmi şəxslər, jurnalistlər, redaktorlar, media direktorları, hüquq müdafiəçiləri,*

xarici beynəlxalq strukturların və Ermənistanda fəaliyyət göstərən xarici ölkə səfirliklərinin əməkdaşlarıdır" (Հակոբյան, 2023).

3. QHT-Lərin Kibertəhlükəsizlikdə Rolu

Ermənistanda kiberinkişaf, kibertəhlükəsizlik məsələləri ilə məşğul olan bir sıra QHT-lər də fəaliyyət göstərməkdədir. Xüsusən, 2019-cu ildən etibarən bu istiqamətdə fəaliyyət göstərən qeyri hökumət təşkilatlarının sayı sürətlə artmaqdadır. Məhz o zamandan beynəlxalq fondlar Ermənistanın İT sektoruna böyük investisiyalar yatırmağa başlamış, bir-birinin ardınca bu ölkədə iri İT şirkətlərinin yeni filialları yaradılmışdı. Bu isə öz növbəsində Ermənistanın İT sektorunda fəallaşmaya, bu sahədə fəaliyyət göstərən QHT-lərin və özəl subyektlərin sayının artmasına gətirib çıxarmışdı (Մարտիրոսյան , 2021).

Hazırda Ermənistanda kibertəhlükəsizlik sahəsində fəaliyyət göstərən QHT-lərdən biri "İSOC Armenia" (Ermənistan İnternet Cəmiyyəti) adlı qeyri-hökumət təşkilatıdır. Rəsmi olaraq "ISOC Armenia" Ermənistanın internet istifadəçilərinin qeyri-kommersiya təşkilatı kimi təqdim olunur. Qeyd edilir ki, yerli internet icması kimi "İSOC Armenia" Ermənistan Milli Elmlər Akademiyasının üzvləri, əsas İnternet provayderləri, universitet və kitabxana şəbəkələri, akademik, tədqiqat və məktəb şəbəkələri, fərdi internet istifadəçiləri və bu istiqamətdə fəaliyyət göstərən hökumət nümayəndələrinin birliyidir. Təşkilatın başlıca məqsədləri sırasında Ermənistanda internetin inkişafına yardım etmək də var.

Beynəlxalq təşkilatların qrantları ilə ISOC Ermənistan erməni məktəbləri üçün 700-ə yaxın şəbəkə administratoru, Ermənistanın regionlarında icma internet mərkəzləri üçün kadrlar hazırlayıb, Ermənistanın regionları üçün avadanlığın saxlanmasına və regional QHT-lərə İT-nin təqdim edilməsinə kömək edən elektron reyderlərin fəaliyyətini təşkil edib.

"İSOC Armenia" fiziki şəxslər, biznes qurumları ilə yanaşı dövlət təşkilatlarına da xidmət göstərir, rəsmi qurumların həyata keçirmək istədiyi bir sıra kiberhücumların həyata keçirilməsinə rəhbərlik edir. "İSOC Armenia" Ermənistanda internet istifadəçilərinə nəzarət etmək üçün hökumətin əlində həm də təməl alətlərdən biridir. Təşkilat internetlə bağlı beynəlxalq konfrans və seminarlarda iştirak üçün üzvlərə səyahət qrantlarının ayırır, internet və şəbəkələşmə üzrə təlimlər təşkil edir, Ermənistanda internet və digər kiber məsələlərlə bağlı aktual problemlərin həlli üçün vəsaitin toplanmasını həyata keçirir. ISOC Ermənistan ".am" və ".հայ" domeinlərinin meneceridir.

ISOC AM Avropa Milli Yüksək Səviyyəli Domen Reyestrləri Şurasının (CENTR) üzvü, Ermənistan İnternet Mübadiləsinin təsisçi üzvüdür. O, həmçinin Asiya-Sakit Okean regionu Yüksək səviyyəli domenlər Asossiasiyasının (APTLD) assosiativ üzvüdür.

Bu sahədə fəaliyyət göstərən başqa bir qurum "ArmSec Fondu"dur. Rəsmi və açıq mənbələrdə göstərilir ki, fond İT, informasiya və kibertəhlükəsizliklə bağlı kurslar, seminarlar, elmi konfranslar və s. kimi inkişaf layihələrini təşkil edir. Bu qurumun təşkil etdiyi tədbirlərdən biri də illik ArmSec konfranslarıdır. Konfransa Ermənistandan olan iştirakçılarla yanaşı, xarici mütəxəssislər də dəvət edilir. Bu toplantılarda Ermənistanda kibertəhlükəsizlik məsələləri və problemlərini müzakirə edilir. Məsələn, 2023-cü ilin noyabrında keçirilən konfransda Ermənistan kibertəhlükəsizlik cəmiyyətinin özəl sektorun rolu, e-gov/gov-tech-in rəqəmsal transformasiyasında iştirakı, Ermənistanın vacib əhəmiyyətli informasiya və kommunikasiya infrastrukturlarının kiberhücumlardan qorunması, informasiya təhlükəsizliyi məsələlərində ictimaiyyətin məlumatlandırılması, təhsil sistemində kibertəhlükəsizlik məsələləri, erməni korporasiyalarına hücumların ransomware növü: mümkün qorunma həlləri və təsirlər, dövlət və özəl təşkilatlara qarşı APT tipli hücumlar, blokçeyn sistemlərində kibertəhlükəsizlik riskləri və kriptoqrafiya kimi məsələlər müzakirə edilmişdi (ArmSec, 2024).

Armsec Fondunun təsisçisi Samvel Martirosyandır. Onun həyatı və fəaliyyəti çoxşaxəlidir. O, İrəvan Dövlət Universitetinin müəllimi, bir çox yerli və xarici media qurumlarının jurnalisti, İT mütəxəssisi, bloqçu, hətta tikinti biznesi sahəsində investor kimi

fəaliyyət göstərib. Ermənistanla Azərbaycan arasında informasiya müharibəsinə dair bir sıra məqalələrin müəllifidir (Martirosyan, 2016). Bu şəxs həm də Ermənistanda Vətəndaş Cəmiyyəti İnstitutlarında İT dəstəyi göstərən CyberHub-AM-ın həmtəsisçilərindən biridir. Bu qurum Təhlükəsizlik təhlilləri aparır, kibertəhlükəsizliklə bağlı kurslar təşkil edir.

2008-ci ilin dekabrında İrəvan şəhərində fəaliyyət göstərən bir qrup həkim və İT mütəxəssisləri tərəfindən yaradılmış "Erməni Rəqəmsal Sağlamlıq Assosiasiyası" Ermənistanda Rəqəmsal Sağlamlığın tədqiqi və inkişaf etdirilməsi istiqamətində fəaliyyət göstərən qeyri-hökumət, qeyri-kommersiya peşəkar təşkilatıdır. Rəsmi açıqlamalarında göstərilir ki, "Erməni Rəqəmsal Sağlamlıq Assosiasiyası"nın başlıca məqsədi yerli səhiyyə sistemində Rəqəmsal Sağlamlıq xidmətlərinin tədqiqi, yaradılması və inkişafı yolu ilə səhiyyənin keyfiyyətini artırmaq və əlçatanlığının təmin edilməsinə nail olmaqdır (Armenian Association of Digital Health. About us, 2024). Təşkilatın ilk sədri professor Georgi Çaltikyan olmuşdur. Qeyd edək ki, Georgi Çaltikyan Bavariyadakı Deggendorf Tətbiqi Elmlər Universitetində Tibbi İnformatika Magistr (MMI) təhsil proqramının direktoru, Almaniya və Erməni Teletibb Assosiasiyasının (AATM) qurucu prezidentidir. Georgi Çaltikyan İrəvan Dövlət Tibb Universitetinin ümumi cərrahiyə ixtisasında təhsil alıb və 15 ilə yaxın klinik praktikada ümumi və laparoskopik cərrahiyyə üzrə təcrübə qazanıb. 2001-2009-cu illərdə İrəvan Dövlət Tibb Universitetinin cərrahiyyə kafedrasında dosent vəzifəsində çalışmış, bakalavr və aspirantlara tibb və cərrahiyyə ixtisaslarından dərs demişdir. 2009-2010-cu illərdə ABŞ-ın Los-Anceles şəhərində Cənubi Kaliforniya Universitetində Fulbrayt Təqaüdçüsü olmuşdur. Bu illər ərzində o, həmçinin Səhiyyə İnformasiya və Kommunikasiya Texnologiyaları (eHealth, Teletibb, Rəqəmsal Sağlamlıq) sahəsində araşdırmalar aparıb. Erməni Teletibb Assosiasiyasının qurucusu olmuşdur. 2019-cu ildə Çaltikyan ÜST-nin Rəqəmsal Sağlamlıq üzrə Ekspertlər Siyahısına daxil edilmişdir.

2023-cü ilin sentyabr ayından etibarən isə "Erməni Rəqəmsal Sağlamlıq Assosiasiyası"na Robin Ohannesyan rəhbərlik edir. Robin Ohannesyan, Fransada Xalq Sağlamlığı üzrə ixtisaslaşmış həkimdir. O, "Télémédecine 360" və "Telemonica" şirkətlərinin həmtəsisçisi və baş icraçı direktoru, Burqon-Franş-Kont Universitetində nevrologiya və insult üzrə tətbiq olunan teletibb üzrə tədqiqatçıdır.

Qeyd etmək lazımdır ki, Ümumdünya Səhiyyə Təşkilatının (ÜST) məlumatına görə, Rəqəmsal Sağlamlıq başlanğıcdan istismara qədər səhiyyənin yaxşılaşdırılması üçün rəqəmsal texnologiyaların inkişafı və istifadəsi ilə bağlı bilik və təcrübə sahəsidir. Başqa sözlə, Rəqəmsal sağlamlıq tibbi şəraiti və sağlamlıq risklərini idarə etmək və insanların rifahını yaxşılaşdırmaq üçün səhiyyədə rabitə və informasiya texnologiyalarından istifadəni nəzərdə tutur. O, geniş əhatə dairəsinə malikdir. Buraya mobil sağlamlıq (mHealth), eHealth, telexidmət, teletibb, sağlamlıq texnologiyası, bioinformatika, tibbi informatika və telesəhiyyə daxildir. Bunlar artıq inkişaf etməkdə olan dünyada səhiyyənin ayrılmaz hissəsinə çevrilib və onların tibbdəki təcrübəsinin inkişaf edəcəyi proqnozlaşdırılır.

Son onilliklərdə xəstəxanalar və ambulatoriyalar xroniki xəstəliklərin yayılmasının artması və bununla əlaqədar olaraq tibbi xidmətə artan tələbatla üzləşmişdir. Halbuki, elektron sağlamlıq qeydləri və böyük məlumatların səhiyyədə tətbiqi tibbi məlumatların getdikcə artan həcmini birləşdirməyə və təhlil etməyə kömək edə bilər.

Nəticə

Beləliklə, aparılan təhlillərdən aydın olur ki, uzun illər ərzində kiberməkanının təhlükəsizliyi heç də normal şəkildə təmin edilməyən Ermənistan son illərdə bu sahənin inkişafına çalışır, bu istiqamətdə fəaliyyət göstərən qeyri-hökumət təşkilatlarının fəaliyyət müxtəlif formalarda dəstəklənir. Burada bir neçə məqsəd güdülür. Ermənistan dövləti qonşu dövlətlərə qarşı yürütdüyü təcavüzkar siyasət kiberməkanda da davam etdirmək üçün aktiv şəkildə qeyri hökumət təşkilatlarından istifadə edir.

ƏDƏBİYYAT

1. *Armenian Association of Digital Health. About us*. (2024). Bu AADH: https://armdigihealth.org/ mənbədən tapılıb
2. *ArmSec*. (2024). Bu Armsec: https://armsec.org/ mənbədən tapılıb
3. *Cybercrime in Armenia*. (2024). Bu Octopus Cybercrime Community – COE: https://www.coe.int/en/web/octopus/-/armenia mənbədən tapılıb
4. *Digital security incidents against the Armenian Civil Society in 2019 – 2020.* (2023). Armenia: Media Diversity Institute.
5. Martirosyan, S. (2016, aprel 07). *Birinci informasiya*. Bu Jam-news: https://jam-news.net/az/birinci-informasiya/ mənbədən tapılıb
6. Դեհերյանը , Ս., & Գեւորգյանը, Ա. (2019, փետրվար 11). *Կիբեռմիջավայրի սպառնալիքները Հայաստանում*. Bu Ամփոփ: https://ampop.am/cyber-security-issues-in-armenia/ mənbədən tapılıb
7. *Կենտրոնի մասին - Համակարգչային Միջադեպերի արձագանքման պետական կենտրոն* . (2024). Առբերված է CERT.AM: https://cert.gov.am/-ից
8. Հակոբյան, Գ. (2023, Նոյամբեր 01). *Aravot.am*. Bu Ամբողջական հոդվածը կարող եք կարդալ այս հասցեով՝: https://www.aravot.am/2023/11/01/1380202/ mənbədən tapılıb
9. Հակոբյան, Գ. (2023, Նոյամբեր 29). *Հայկական դասագրքերի QR կոդերը տարել են թուրքական դրոշով կայք, ըստ ԿԳՄՄՆ պաշտոնյայի՝ ոչինչ 100%-ով պաշտպանված չի լինել չի կարող*. Bu Aravot: https://www.aravot.am/2023/11/29/1385448/ mənbədən tapılıb
10. Հակոբյան, Գ. (2023, Նոյամբեր 29). *Հայկական դասագրքերի QR կոդերը տարել են թուրքական դրոշով կայք, ըստ ԿԳՄՄՆ պաշտոնյայի՝ ոչինչ 100%-ով պաշտպանված չի լինել չի կարող*. Bu Aravot.am: https://www.aravot.am/2023/11/29/1385448/ mənbədən tapılıb
11. Մարտիրոսյան , Ս. (2021, սեպտեմբեր 23). *Երկրորդ Էշելոնի սոցիալական մեդիան Հայաստանում*. Bu Media.am: https://media.am/hy/critique/2021/09/23/29592/ mənbədən tapılıb
12. Մելքոնյան, Թ. (2024, փետրվար 02). *Կառավարությունը ձախողել է կիբեռանվտանգության ռազմավարական ծրագիրը. ու՞մ մեղքով չի ստեղծվել ԱԿԳ կենտրոնը* . Bu News.am: https://news.am/arm/news/805331.html mənbədən tapılıb