Tənqidçilərin onlayn hüquqlarına kiber hücumlarda Azərbaycan nümunəsi: qanunvericilikdə və təcrübədə çatışmazlıqlar, hücumların siyasi mənası

I. Giriş

Son illərdə dünyada əsasən insan hüquq müdafiəçiləri, demokratiya aktivistləri, siyasi və ictimai fiqurlar, jurnalistlər və internet medialarını hədəf alan kiber hücumların yüksələn trendi müşahidə olunur. Bu hücumlar əsasən hədəf alınan şəxslərin ifadə, fərdi məlumatların toxunulmazlığı, məlumata çatımlılıq kimi fundamental insan hüquqlarını onlayn məkanda pozur. Narazı səslərə qarşı onlayn hücumların son illərdə geniş vüsət aldığı Azərbaycan da bu trenddə mənfi mənada pay sahibidir. Əksər hallarda casus proqramları, fişing və DDoS hücumları və şifrələrin oğurlanması ilə müşayiət olunan kiber əməliyyatlar insanlar və təşkilatların fərdi məlumatlarının, onlayn hesablarının icazəsiz ələ keçirilməsi, paylaşılması, onlar vasitəsilə şantaj olunma, sosial media platformalarında paylaşımların və izləyicilərin silinməsi, cihazların sıradan çıxarılması kimi ağır mənfi nəticələrə səbəb olur. Bir sıra hallarda isə müxtəlif araşdırmalar bu hücumların mənbəyində hökumət və ya hökumətə yaxın qrup və şirkətlərin iştirakına işarə edir. Belə olan halda kiber hücumlardan qorunmaq üçün səmərəli hüquqi şəraitin və siyasət tədbirlərinin mövcudluğuna xüsusi ehtiyac yaranır. Bu yazı Azərbaycanda kiberhücumlarla mübarizəni qanunvericilikdə çatışmazlıqlar, istintaq tədbirlərinin səmərəliliyi və hücumların mümkün siyasi xarakteri fonunda təhlil edir.

İlk bölmədə ilkin anlayışlar və Azərbaycanda kiber hücumlara ilkin statistik göstəricilər təqdim olunur. Daha sonra Azərbaycanda kiber təhlükəsizlik sahəsində milli qanunvericiliyin cari vəziyyəti müzakirə olunur, çatışmazlıqlar beynəlxalq və regional insan hüquqları sənədləri və Avropa İnsan Hüquqları Məhkəməsinin (AİHM – bundan sonra) presedent hüququnun (*ing: case law)* fonunda təhlil olunur. Bir sonrakı bölmədə isə Azərbaycanda tənqidçilərə qarşı kiber cinayət hallarına dair istintaq tədbirlərinin səmərəliliyi müzakirə olunur. Növbəti bölmədə əvvəlcə azərbaycanda kiber hücumlara dair statistika incələnir, sonra isə kiber hücumların siyasi əhəmiyyəti hücumlarla zərərçəkənlərin insan hüquqları fəaliyyəti arasında əlaqə əsas götürülərək araşdırılır. Son bölmədə isə kiber hücumların insan hüquqlarına təsiri və onlardan müdafiəyə dair qanunvericilik və təcrübədə çatışmazlıqlara dair ümumiləşdirici fikirlər yer alır.

Bu bloq yazısı insanların internet azadlıqlarına yönəlmiş kiber hücumları *Azərbaycan kontekstində və fərdi məlumatların qorunması ilə bağlı məsələlərə fokuslanaraq təhlil edir.* Yazının ana xətti əsasən insan hüquq müdafiəçiləri, vətəndaş cəmiyyəti fəalları, jurnalistlər və media qurumlarının timsalında tənqidçilərə yönəlik onlayn hücumlar, hücumlara qarşı hüquqi təminatların mövcudluğu və fərdi məlumatların qorunması ilə əlaqədar qanunvericiliyin vəziyyəti ətrafındadır. Yazının əsas xətti və həcmi ilə bağlı gözləntiləri nəzərə alaraq müəllif kiber hücumların bizneslər və digər hüquqi şəxsləri, o cümlədən dövlətləri hədəf alan formalarına toxunmur.

II. İlkin anlayışlar, Azərbaycanda kiber hücumlara ümumi baxış

İnsan hüquqlarının insanlara doğulduqları andan, qeyd-şərtsiz və bərabər qaydada təmin olunması prinsipi internetdən istifadənin getdikcə populyarlaşdığı dövrdə hüquq və azadlıqların onlayn məkanda da qorunmasını şərtləndirir. Bu mənada dövlətlərin insanların hüquqlarını pozmamaq, qorumaq və tam həyata keçirməyə yönəlik öhdəlikləri müvafiq olaraq onlayn məkana da tərcümə olunur. Təsadüfi deyil ki, Beynəlxalq Millətlər Təşkilatının İnsan

Hüquqları Şurasının 2012-ci ildə qəbul etdiyi qətnamədə də insan hüquqlarının avtomatik olaraq onlayn məkanda da eyni qaydada qorunmalı olduğu bəyan edilib.[1]

İnternet azadlıqları dedikdə insanların əsasən ifadə, məlumat, sərbəst toplaşma və birləşmə azadlıqları və şəxsi və ailə həyatına hörmət hüquqları ilə əlaqəli təminatları nəzərdə tutulur. Belə ki, bu azadlıqlar müvafiq olaraq internet və onlayn məzmuna çatımlılıq, azad informasiya mübadiləsi, fərdi məlumatların onlayn məkanda gizliliyi və qorunması və bu hüquqlardan istifadə zamanı təzyiq, hədə və hücumlardan qorunma kimi təminatları yaradır.[2] Bəzi mənbələrsə internetdə azadlıqları daha geniş şərh edir.[3] *Tənqiçdilərə münasibətdə isə əsasən fərdi məlumatların onlayn məkanda qorunması ilə əlaqədar məsələlər xüsusilə önə çıxır.*

Kiber hücumlar müxtəlif informasiya və kompüter texnologiyaları vasitəsilə informasiya sistemləri, cihazlar və dolayısı ilə fərdi və bəzən dövlət əhəmiyyətli məlumatlara icazəsiz müdaxilə, ələ keçirilmə, silinmə, dəyişdirilmə və ya paylaşılması kimi anlayışları ifadə edir. Xakinq məlumat və sistemlərə icazəsiz müdaxilə və ələ keçirmənin ümumi adıdır. Ona SMS-lərə müdaxilə ilə və ya kobud gücün (*ing: brute force*) tətbiqi ilə şifrələrin ələ keçirilməsi daxil olmaqla onlarla üsul daxildir. Fişinq hücumları isə daha konkret istifadəçinin adətən email, zəng, mesaj və ya digər vasitələrlə tələyə düşüb şəxsi məlumatlarını ələ verməsini ilə baş verir. Belə hücumlarda istifadəçiyə dair şəxsi məlumat, onlayn hesab və ya ümumilikdə viruslu proqrama yoxluma vasitəsilə cihazın ələ keçirilməsi kimi nəticələr ola bilər. DDoS hücumları zamanı isə xüsusi texniki vasitələrin köməyi ilə onlayn informasiya ehtiyatına kütləvi giriş həyata keçirilir və beləliklə həmin informasiya ehtiyatına sadə istifadəçilərin girişi məhdudlaşdığı üçün faktiki olaraq xidmətdən istifadə mümkünsüzləşir. Kiber hücumlara eyni zamanda kiber bullinq və zorakılığı və onlayn identifikasiya məlumatlarının oğurlanmasını da nümunə vermək olar. İdentifikasiya Məlumatlarının Oğurlanması – istifadəçilərə dair, onların kimliyi ilə bağlı məlumatların ələ keçirilməsi yolu ilə onların onlayn təqlidini və onların adlarından əməliyyat və hərəkətlər həyata keçirilməsini nəzərdə tutur. Kiber bullinq və zorakılığa isə onlayn platformalarda insanlara dair yalanlar yaymaq, onları utandırmaq və ya qorxutmaq üçün şəkil və məlumatlarını icazəsiz paylaşmaq, davamlı olaraq təhdid və zərərli mesajlar ünvanlamaq, onları təqlid edərək başqaları ilə ünsiyyətə girməyi misal çəkmək olar. Gözləmək olar ki, texnologiya inkişaf etdikcə bu hücumların da növ və mürəkkəbliyi artacaq. Bu hücumlara qarşı insan hüquqlarını qorumaq üçün müxtəlif ölkələr və təşkilatlar ötən əsrin sonlarından etibarən kiber təhlükəsizliyə dair qanun və siyasət tədbirləri çərçivəsində önləm alırlar.

Azərbaycanda da kiber hücumların son illərdə qarşı artan xətti müşahidə olunur. Belə ki, təkcə 2018-ci ildən etibarən, son 5 ildə ən az 46 halda insan hüquq müdafiəçiləri, aktivistlər, siyasətçilər, jurnalistlər, internet mediaları və digər tənqidçilərə qarşı kiber hücumlara dair informasiyalar mediada yer alıb.[4] Bu işlərdə əsasən yuxarıda adı keçən qrupa aid şəxs və təşkilatların onlayn hesabları DDoS və fişinq hücumları, virus yoluxdurulması, məxfi sözlərin

[1] Birləşmiş Millətlər Təşkilatı (BMT), 'Internetdə insan hüquqlarının təbliği, müdafiəsi və onlardan faydalanma: İnsan Hüquqları Şurası tərəfindən qətnamə', (2012), A/HRC/20/L.13, para 1, https://digitallibrary.un.org/record/731540?ln=en,

[2] Avropa Şurası Nazirlər Komissiyası, 'Nazirlər Komitəsinin üzv dövlətlərə internet azadlıqları ilə bağlı tösviyələri', (2016), CM/Rec(2016)5[1], paras. 1-5, https://freedomhouse.org/reports/freedom-net/freedom-net-research-methodology

[3] BMT-nin Insan Hüquqları üzrə Ali Komissarlığı, 'İnternet üçün İnsa Hüquqları və Prinsiplərinin Xartiyası', (2014), səhifə 9, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf

[4] Ətraflı məlumat üçün bax: 1 nömrəli qoşma

ələ keçirilməsi və s. yollarla ələ keçirilib, onlara dair fərdi məlumatlar oğurlanıb, silinib, şantaj predmeti kimi istifadə olunub və bəzi hallarda isə icazəsiz olaraq paylaşılıb. Ən azı 8 halda isə hücumların arxasında Daxili İşlər Nazirliyi (DİN – bunda sonra), Dövlət Təhlükəsizlik Xidməti (DTX – bundan sonra) və digər qurumların timsalında Azərbaycan hökumətinin yer aldığı iddia olunub.[5] Bundan başqa qeyd etmək lazımdır ki, bəzi hallarda bu kiber hücumlar hətta dövlət əhəmiyyətli qurumlara yönəlib.[6]

III. Milli qanunvericilikdə internet azadlıqlarına kiber hücumlara qarşı hüquqi təminatlar və çatışmazlıqlar

1. *Azərbaycanda tənqidçilərin internet azadlıqlarına yönələn kiber hücumlara qarşı hüquqi təminatlar*

Azərbaycanda internet azadlıqlarının təmin olunması üçün bir sıra qanunvericilik təminatları mövcuddur. Belə ki, həm Azərbaycan Respublikasının Konstitusiyası, həm də Azərbaycanın tərəfdaş çıxdığı beynəlxalq və regional insan hüquqları sənədləri – Birləşmiş Millətlər Təşkilatnın (BMT – bundan sonra) "Mülki və Siyasi Hüquqlar haqqında Beynəlxalq Pakt"-ı və "İnsan hüquq və əsas azadlıqların müdafiəsi haqqında'" Avropa Şurasının (AŞ – bundan sonra) Konvensiyası (AİHK – bundan sonra) internet azadlıqlarının kökündə duran ifadə, sərbəst toplaşma, məlumat və şəxsi və ailə həyatına hörmət azadlıqlarını tanıyır.[7] Xüsusilə də Konstitusiyanın 32-ci maddəsi fərdi məlumatların qorunması çərçivəsində insanların telefon, poçt və digər vasitələrlə ötürülən məlumatlarının məxfiliyinə hüquqi təminat yaradır.[8]

Bundan başqa Azərbaycan 2001-ci ildə "Kibercinayətkarlıq haqqında" Budapeşt Konvensiyasına tərəfdaş çıxaraq ratifikasiya edib.[9] Bu isə müvafiq olaraq AİHK ilə oxşar olaraq məcburedici xarakter daşıyır və Azərbaycanın qarşısında milli qanunvericiliyin konvensiyaya uyğunlaşdırılması, o cümlədən kiber hücumlara dair cinayət məsuliyyəti yaratmaq, onlayn məzmunun tənzimlənməsi ilə bağlı qanunlar qəbul etmək və kiber cinayətlərin qarşısını almaq üçün beynəlxalq əməkdaşlıqla bağlı öhdəliklər yaradır.

---

[5] Qurium Media Foundation, 'Azerbaijan and the Fineproxy Diy Ddos Service (Region40 / Qualitynetwork)', (2018), https://www.qurium.org/alerts/azerbaijan/azerbaijan-and-the-region40-ddos-service/;
Qurium Media Foundation, 'Finding Man; the Phisher of Journalists in Azerbaijan', (2020), https://www.qurium.org/alerts/azerbaijan/finding-man-the-phisher-of-journalists-in-azerbaijan/;
Azerbaijan Internet Watch (AIW), 'targeted harassment via telegram channels and hacked Facebook accounts' (2021), https://www.az-netwatch.org/news/targeted-harassment-via-telegram-channels/;
PHR-AIW, 'Pulling the plug: How Azerbaijan's government combines technology and fear to control the internet', (2021), p 32, https://www.iphronline.org/wp-content/uploads/2021/09/Pulling-the-Plug_report_updated_compressed-1.pdf; (IPHR Report)
AIW, 'Another phishing attempt', (2020), https://www.az-netwatch.org/news/another-phishing-attempt/ ;
Ətraflı məlumat üçün bax: 1 nömrəli qoşma

[6] MeydanTV, 'Icbari Sığorta Bürosuna Hücum: 40 milyondan çox məlumat oğurlanıb', (2022), https://www.meydan.tv/az/article/icbari-sigorta-burosuna-kiberhucum-40-milyondan-cox-melumat-ogurlanib/

[7] BMT Baş Assambleyası', 'Mülki və Siyasi Hüquqlar Haqqında Beynəlxalq Pakt', (16 Dekabr 1966), BMT Müqavilələr seriyası, cild 999, səhifə 171, Maddələr 17,19,22;
AŞ, 'Insan Hüquqları və Əsas Azadlıqların Müdafiəsi Haqqında Avropa Konvensiyası', (4 Noyabr 1950), ETS 5, Maddələr 8, 10, 11; (AİHK)

[8] Bax: E-qanun.az, 'Azərbaycan Respublikasının Konstitusiyası', (12 Noyabr 1995), Maddə 32, https://www.e-qanun.az/framework/897; (Konstitusiya)

[9] E-qanun.az, 'Kibercinayətkarlıq haqqında Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu', (2009), № 874-IIIQ, https://e-qanun.az/framework/18619

Milli qanunvericilikdə isə kiber təhlükəsizlik sahəsində münasibətləri tənzimləyən vahid qanuna rast gəlinməsə də, internet azadlıqlarını, xüsusilə də fərdi məlumatların mühafizəsi ilə əlaqəli əsas qanunlara Azərbaycan Respublikasının "Fərdi Məlumatlar haqqında",[10] "İnformasiya, İnformasiyalaşdırma və İnformasiyanın Mühafizəsi haqqında",[11] "Telekommunikasiya haqqında",[12] "Dövlət Sirri haqqında"[13] və "Əməliyyat-axtarış fəaliyyəti haqqında"[14] qanunları aiddir. Bundan başqa Azərbaycan Respublikasının Cinayət Məcəlləsi (CM – bundan sonra) və Cinayət Prosessual Məcəlləsinin (CPM – bundan sonra) müvafiq bölmələri və Nazirlər Kabinetinin bir neçə qərarı da bu sahədə münasibətlərin tənzimlənməsinə xidmət edir. Bu qanunlar və normativ hüquqi aktlar birlikdə müxtəlif anlayışlara tərif verir, fərdlərin, hüquqi şəxslərin və dövlətin öhdəliklərini, hüquqlarını və müvafiq məhdudiyyət və sanksiyaları müəyyən edir.

2. *Beynəlxalq hüquqda kiber hücumlardan müdafiəyə dair qanun və sənədlərin ümumi vəziyyəti*

İnternet azadlıqlarına artan kiber hücumlara baxmayaraq beynəlxalq səviyyədə hələ də kiber təhlükəsizliyə dair vahid insan hüquqları sənədinə rast gəlinmir. BMT nəzdində müxtəlif dövrlərdə bu yöndə qanun layihələri müzakirəyə çıxarılsa da yekun sənəd hələ ki, yoxdur. Regional qurumlarsa bu baxımdan daha çevik davrana biliblər. Belə ki, kiber təhlükəsizlik sahəsində ən təkmil və məcburedici xarakterə malik konvensiya AŞ-ın 2001-ci ildə qəbul etdiyi və bütün dünya üzrə 68 ölkə tərəfindən dəstəklənən "Kiber cinayətkarlıq haqqında" Budapeşt Konvensiyasıdır. Konvensiya ölkələr qarşısında milli qanunvericilikdə kompüter sistemləri və məlumatlara yönəlmiş hücumlar və məzmunla bağlı pozuntulara dair cinayət məsuliyyəti yaradaraq mübarizə aparmaq öhdəliyi qoyur və kiber cinayətlərin qarşısının alınması üçün beynəlxalq əməkdaşlıq mexanizmi ilə çıxış edir. Avropa İnsan Hüquqları Məhkəməsi (AİHM – bundan sonra) də son illərdə internet azadlıqları və kiber hücumlara dair presedent hüququnu inkişaf etdirməyə davam edir. İnternet azadlıq Bundan başqa bir neçə başqa regional qurumlar da kiber cinayətkarlığa dair konvensiyalarla çıxış ediblər.[15]

Avropa İttifaqı məkanından 2018-ci ildən qüvvəyə minən 'Ümumi Məlumatın Mühafizəsi Qaydaları' (GDPR – bundan sonra) isə fərdi məlumatların mühafizəsi sahəsində regionun ən təkmil və məcburi xarakter daşıyan sənədi hesab olunur və hüquqi şəxslərin məlumatlarıa davranış qaydaları ilə bağlı öhdəliklərinin müəyyən olunmasında hərtərəfliliyi ilə seçilir.[16] Eyni zamanda 37 ölkənin üzv olduğu 'Freedom Online Coalition' hökumətlərarası koalisiyası da internet azadlıqlarının qorunması və kiber təhlükəsizlik sahəsində vahid beynəlxalq standartların yaranması üçün ortaq, bələdçi xarakterli bəyanatlarla çıxış edir.[17]

---

[10] E-qanun.az, 'Fərdi məlumatlar haqqında', (2010), 998-IIIQ, https://e-qanun.az/framework/19675
[11] E-qanun.az, 'Informasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikasının Qanunu', (1998), № 460-IQ, https://e-qanun.az/framework/3525
[12] E-qanun.az, 'Telekommunikasiya haqqında Azərbaycan Respublikasının Qanunu', (2005), № 927-IIQ, https://e-qanun.az/framework/10663; (Telekommunikasiyalar haqqında qanun)
[13] E-qanun.az, 'Dövlət Sirri haqqında Azərbaycan Respublikasının Qanunu', (2004), № 733-IIQ, https://e-qanun.az/framework/5526
[14] E-qanun.az, 'Əməliyyat-axtarış fəaliyyəti haqqında Azərbaycan Respublikasının Qanunu', (1999), № 728-IQ https://www.e-qanun.az/framework/2938 (Əməliyyat-axtarış fəaliyyəti haqqında qanun)
[15] African Union, 'African Union Convention on Cyber Security and Personal Data Protection', (27 June 2014), https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection;
[16] European Union, 'General Data Protection Regulation', (2016), (EU) 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj
[17] Freedom Online Coalition, 'Joint Statements', (2023), https://freedomonlinecoalition.com/joint-statements/

Beynəlxalq vətəndaş cəmiyyəti təşkilatları isə internet azadlıqlarının qorunması və kiber hücumlardan müdafiəyə dair normaların müəyyənləşdirilməsi üçün kampaniyanın ən aktiv iştirakçılarıdır. İnsan hüquqları, məxfilik (privatlıq) və təhlükəsizlik üzrə ixtisaslaşmış onlarla təşkilat və ekspertin hazırladığı, 400-dən çox təşkilatın və 350000-dən çox fərdin imzalayaraq qoşulduğu 'Kommunikasiyaların İzlənməsində İnsan Hüquqlarının Tətbiqinə dair Beynəlxalq Prinsiplər' sənədi dünyada internet azadlıqlarının daha yaxşı qorunması üçün qanunvericilik tədbirlərinə istiqamət verəcək 13 prinsipi əhatə edir.[18] Hökumətlərin izləmə və dinləməyə imkan verən texnologiyalardan istifadəsinin artmasının fonunda sənəd beynəlxalq insan hüquqları prinsiplərinin dövlətlər üçün digital məkanda hansı öhdəlikləri yaratdığını ifadə edir və məcburedici xarakter daşımasa da mötəbər mənbə kimi müsbət inkişafa töhfə verir.

3. *Azərbaycanda milli qanunvericiliyin beynəlxalq standartlarla müqayisədə çatışmazlıqları*

İzləmə və dinləmə təbirlərində qeyri-dəqiq standartlar və hüquq-mühafizə orqanlarının qeyri-proporsional səlahiyyətləri

Onlayn azadlıqların təmin olunmasında fərdi məlumatlarının qorunması xüsusi önəm daşıyır. Bu hüquqdan faydalanma zamanı isə ən böyük hədələrdən biri informasiya-kompüter texnologiyaları vasitəsilə izləmə və dinləmə (*ing: surveillance*) tədbirləri ilə bağlıdır. Bu insanlara dair fərdi məlumatların müxtəlif vasitələrlə müəyyən məqsədlər uğrunda güdülməsi ilə bağlı anlayışdır. Nüfuzlu beynəlxalq insan hüquqları təşkilatlarının araşdırmaları göstərir ki, hətta kütləvi xarakter də daşıya bilən bu tədbirlər əksər hallarda insan hüquqlarını hədə altında qoyur və tez-tez avtoritar rejimlər tərəfindən tənqidçilərin izlənilməsi üçün sui-istifadə olunur.[19] Bu mənada izləmə və dinləmə tədbirlərinə qarşı hüquqi təminatların mövcudluğu insan hüquqlarının o cümlədən internet azadlıqlarının qorunması baxımından vacib hesab olunur və beynəlxalq hüquq-müdafiə təşkilatları və o cümlədən BMT və AŞ tərəfindən diqqətdə saxlanılır.

Roman Zaxarov Rusiyaya qarşı işi-nin timsalında AİHM-nin presedent hüququ fərdə dair şəxsi məlumatların dinlənilməsi və izlənilməsini şəxsi həyatın toxunulmazlığı hüququna ciddi müdaxilə hesab edir və bütün məhdudiyyətlərin qanunla dəqiq müəyyən edilmiş formada olmasına, legitim məqsədə cavab verməsinə və demokratik cəmiyyətdə bu məqsədə çatmaq üçün zəruri olmasına diqqət yetirir.[20] Azərbaycanda Konstitusiyanın 32-ci maddəsi digər qanunlarla birlikdə fərdlərin şəxsi məlumatlarının qorunmasına təminat verir, qanunsuz müdaxilə hallarında görə inzibati və cinayət məsuliyyəti müəyyən edilir.[21] Bununla belə bu hüquq mütləq hesab olunmur və qanunla göstərilən hallarda və məhkəmə qərarı ilə məhdudiyyətə məruz qala bilər.

---

[18] Electronic Frontier Foundation, 'Necessary and Proportionate', (2013), https://www.eff.org/files/necessaryandproportionatefinal.pdf, (13 Prinsip)

[19] BMT-nin Insan Hüquqları üzrə Ali Komissarlığı, 'Digital dövrdə məxfilik hüququ', (2022), A/HRC/51/17, para 53, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement

[20] *Roman Zaxarov Rusiyaya qarşı işi*, №. 47143/06, (2015 AIHM), para. 227;

[21] Bax: Konstitusiya, Maddə 32;
"Hər kəsin yazışma, telefon danışıqları, poçt, teleqraf və digər rabitə vasitələri ilə ötürülən məlumatın sirrini saxlamaq hüququna dövlət təminat verir."
E-qanun.az, 'Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsi', (2015), 96-VQ, Maddələr: 375.0.2, 388-1, https://www.e-qanun.az/framework/46960;
E-qanun.az, 'Azərbaycan Respublikasının Cinayət Məcəlləsi', 32(1999), 787-IQ, Maddələr: 155, 156.1, https://www.e-qanun.az/framework/46947

Belə ki, "Əməliyyat-axtarış fəaliyyəti haqqında" qanuna və CPM-ə əsasən digər tədbirlərlə yanaşı insanların telefon, poçt və digər rabitə kanalları vasitəsilə ötürdükləri məlumatların izlənilməsi yalnız qanunla müəyyən olunmuş qaydada və məhkəmə təsdiqi ilə mümkündür.[22] Ancaq, qanunun 10-cu maddəsinin dördüncü hissəsi şəxsiyyət əleyhinə ağır cinayətlərin və ya xüsusi təhlükəli dövlət cinayətlərinin qarşısının alınması məqsədilə məhkəmə qərarı olmadan belə müstəntiqin əsaslandırılmış qıraarı ilə hüquq-mühafizə orqanlarına şəxsiyyət əleyhinə ağır cinayətlərin və ya xüsusi təhlükəli dövlət cinayətlərinin qarşısının alınması üçün məhkəmə qərarı olmadan belə telefon danışıqlarına qulaq asmağa və texniki rabitə kanallarından və digər texniki vasitələrdən məlumatları çıxarmağa icazə verir.[23] Lakin qanunvericiliyin təhlili göstərir ki, qanunvericilik Lakin milli qanunvericilik izləmə və dinləmə tədbirləri vasitəsilə əldə edilmiş fərdi məlumatların hansı müddətdə saxlanılması və məhv edilməsinə dair standartlar müəyyənləşdirməyib. Bu isə müvafiq olaraq hüquq-mühafizə orqanlarına əldə olunmuş fərdi məlumatlarla davranışla bağlı ölçüsüz sərbəstlik tanıyır.

AİHM cinayət-axtarış tədbirləri çərçivəsində izləmə və dinləmə hadisəsinə münasibətdə, o cümlədən *Huviq Fransaya qarşı işində* bildirir ki, bu hallar şəxsi həyata hörmət hüququna ciddi müdaxilə olduğu üçün təznimləyici qanunlar xüsusilə dəqiqliklə işlənilməlidir.[24] Belə ki, məhkəmə dinləmə və izləmə tədbirlərinin insan hüquqlarını pozmaması üçün bir sıra hüquqi təminatlar arasında əldə olunmuş məlumatın istifadəsi, saxlanılması və məhv edilməsinə dair dəqiq və aydın standartların olmasını şərt hesab edir.[25]

Hüquq-mühafizə orqanlarının izləmə və dinləmə tədbirlərinə və kiber hücumlara qarşı səmərəli şikayət mexanizmlərinin mövcudluğu

AİHK-nın 13-cü maddəsi insanların səmərəli müdafiəsi vasitəsilə ilə təmin olunma hüququnu təsbit edir.[26] Bu maddə AİHK-qeyd olunan hüquq və azadlıqların, o cümlədən internet azadlıqlarının pozulması zamanı insanların səmərəli hüquq müdafiəsi hüququ təmin olunmalı, başqa sözlə pozulan hüquqdan şikayət vermək mümkün olmalı və şikayətə səmərəli qaydada baxaraq qərar verə biləcək mexanizmlər mövcud olmalıdır.[27]

Dinləmə və izləmə tədbirləri ilə bağlı qanunvericilikdə dəqiqliyin çatışmaması, başqa sözlə hüquq-mühafizə orqanlarına ölçüsüz səlahiyyət tanınması insanların pozuntu hallarından səmərəli müdafiə hüququnu da təhlükə altında qoyur.

İstifadəçilərin məlumatlandırılması prinsipinə ilk növbədə vətəndaşların hansı hallarda və hansı şərtlər altında izlənə bilinəcəklərinə dair kifayət qədər məlumatlandırılması daxildir. Belə

[22] E-qanun.az, 'Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi', (2000), 907-İQ, Maddə: 177.3.5, 443, 445, https://www.e-qanun.az/framework/46950; (Cinayət-Prosessual Məcəlləsi); Əməliyyat-axtarış fəaliyyəti haqqında qanun, Maddə 10

[23] Cinayət-Prosessual Məcəlləsi, Maddə 177, 443, 445; Əməliyyat-axtarış fəaliyyəti haqqında qanun, maddə 10; Abbasov E., 'Azərbaycanda Onlayn Məkanda Şəxsi Həyatın Toxunulmazlığı', (2022), AIW, https://aihmaz.org/az%C9%99rbaycanda-onlayn-m%C9%99kanda-s%C9%99xsi-h%C9%99yatin-toxunulmazligi-emin-abbasov/#_edn18; (Abbasov AIW)

[24] *Huviq Fransaya qarşı işi,* №. 11105/84 (1990 AİHM), para 32; AİHM, 'İnsan Hüquqları üzrə Avropa Konvensiyasının 8-ci maddəsinə dair bələdçi', (2022), para. 603, https://www.echr.coe.int/documents/guide_art_8_eng.pdf; (Maddə 8 Bələdçi)

[25] *Karabeyoğlu Türkiyəyə qarşı işi,* №. 30083/10, (2016 AİHM), para 69;

[26] AİHK, maddə 13

[27] *Kaya Türkiyəyə qarşı işi*, №. 22729/93, (1998 AİHM), paras. 106-7; Abbasov AIW (n23);

ki, *Klass və başqaları Almaniyaya qarşı* işində qeyd olunur ki, müşahidə altında olan şəxslərin bundan xəbərsiz olmaları və avtomatik olaraq şikayət etmək imkanlarının olmamaları onların həm yerli, həm də Konsensiya səviyyəsində hüquqları müdafiə mexanizmlərindən məhrum olmalarına səbəb ola bilər.[28] Ancaq izləmə və dinləmə tədbirlərinin vətəndaşlara əlçatan qanun formasında olması hələ pozuntuya qarşı səmərəli mexanizm hesab oluna bilməz. Çünki, məhkəmə *Roman Zaxarov Rusiyaya* qarşı işində xüsusilə qeyd edir ki, bəzən "məxfi müşahidə tədbirlərinin və ya belə tədbirlərə icazə verən qanunvericiliyin mövcudluğu səbəbindən də pozuntu qurbanı olduğunu iddia bilər".[29]

Başqa sözlə kiber cinayətkarlığa qarşı insan-əsaslı yanaşmanın prinsiplərindən biri olan istifadəçilərin məlumatlandırılması prinsipinə əsasən vətəndaşlar onların izləmə və dinləmə tədbirlərinin mümkünlüyü ilə bağlı xəbərdar edilməli və ya bundan şikayət vermə imkanına malik olmalıdılar.[30] Baxmayaraq ki, bəzi hallarda bu kimi xəbərdarlıq istintaqın səmərəsini və nəticəsini sual altında qoya bilər, AİHM presedent hüququnda, o cümlədən *Roman Zaxarov Rusiyaya qarşı işi*-ndə qeyd edir ki, izləmə və dinləmə tədbirləri təbiət etibarilə gizlilik tələb etsə də vətəndaşların sərəncamında sui-istifadə hallarından qorunmaq zəruri hüquqi müdafiə mexanizmləri mövcud olmalıdır.[31] Yəni, qanunvericilik prosesin hər hansı mərhələsində

Azərbaycanda CPM cinayət təqibi ilə bağlı izləmə və dinləmə tədbirlərinə cəlb oluna biləcək şəxslərin kimliyini kifayət qədər dar çərçivədə (təqsirləndirilən və şübhəli şəxslər olmaqla)[32] müəyyən etsə də həmin şəxslərə bu hallardan şikayət verməkdə səmərəli mexanizmlərin mövcudluğu sual altındadır. Belə ki, CPM-də və fərdi məlumatların toxunulmazlığı ilə bağlı əlaqədar qanunlarda dinləmə, izləmə tədbirlərinə məruz qalan şəxslərin ictimai şəkildə əlçatan olan qanunun varlığından əlavə prosesin hər hansı mərhələsində bundan xəbərdar edilmələri ilə bağlı qeydlərə rast gəlinmir. CPM-nin 19-cu maddəsində təqsirləndirilən və ya şübhəli bilinən şəxslərin hüquqi yardım almaq və müdafiə hüququndan yararlanmaları ilə bağlı müddəaları arasında onlara hüquqlarının izah olunması ilə bağlı müddəa yer alır.[33] Bu müddəanın daha dəqiq redaktəsi və ya təcrübədə yeni yanaşmanın tətbiqi vasitəsilə bu hüquqların izah prosesində onların həmçinin mümkün izləmə və dinləmə tədbirlərinə cəlb oluna biləcəkləri ilə bağlı xəbərdarlıq verilə, o cümlədən sonradan şikayət etmək imkanlarına dair məlumatlar təqdim oluna bilər. Eyni zamanda qanunvericiliyə keçmişdə aparılmış və nəticə verməmiş izləmə və dinləmə tədbirləri barədə müəyyən zaman aşımından sonra izlənilmiş şəxslərə məlumat təqdim olunması halı da nəzərə alına bilər. Bu fürsətlərin yoxluğundan vətəndaşlar izləmə və dinləmə tədbirlərinə məruz qalsalar da bundan xəbərdar olmadıqları üçün avtomatik qaydada mümkün hüquq pozuntusundan şikayət vermə imkanından və dolayısı ilə AİHK-in 13 maddəsi ilə təmin olunan səmərəli müdafiə hüququndan məhrum olmuş olurlar.

İzləmə və dinləməyə imkan verən mexanizmlərin satınalınması ilə bağlı şəffaflığın təmin olunması

Daha öncə bəhs edildiyi kimi, dinləmə və izləmə tədbirləri şəxsi həyatın toxunulmazlığı ilə əlaqəli hüquqlara kobud müdaxilə hesab edildiyi üçün onun sui-istifadəsi ehtimalına qarşı milli

[28] *Klass və başqaları Almaniyaya qarşı işi,* № 5029/71 (1978 AİHM), para 36; Abbasov AIW (n23)
[29] *Roman Zaxarov Rusiyaya qarşı işi*, №. 47143/06, (2015 AIHM), paras. 171-2; Abbasov AIW (n23)
[30] Maddə 8 Bələdçi (n24), para 604
[31] *Roman Zaxarov Rusiyaya qarşı işi*, №. 47143/06, (2015 AIHM), paras.233; Maddə 8 Bələdçi (n24), paras 603-5
[32] Cinayət Prosessual Məcəllə, maddə 259.1
[33] Cinayət Prosessual Məcəlləsi, maddə 19.4.2

qanunvericilikdə əhəmiyyətli hüquqi təminatlar yer almalıdır. BMT-nin fikir və ifadə azadlığı üzrə xüsusi məruzəçisinin İnsan Hüquqları Şurasına 2019-cu ildə təqdim etdiyi hesabatda da bu məsələyə toxunulur. Məruzəçi qeyd edir ki, təcrübə göstərir ki, hökumətlərin izləmə və dinləməyə imkan verən texnoloji vasitələrdən yararlanmasına qarşılıq hüquqi təminat kimi səlahiyyətli məhkəmə tərəfindən icazə verilməsi tələb olunsa da bu kifayət deyil.[34] Bu qənaətə gəlmək üçün səbəb kimi göstərilməsə də məruzəçi eyni hesabatda bildirir ki, nadir hallarda izləmə və dinləmə qurbanları milli səviyyədə hüquqi iddialarla uğur əldə edə bilirlər.[35]

Hesabatda əlavə hüquqi təminat kimi isə izləmə və dinləməyə imkan verən texnika vasitələrlə bağlı dövlət satınalmalarında ictimai nəzarətin və şəffaflığın təmin olunması təklif olunur. Beynəlxalq təcrübəyə əsasən iddia olunur ki, yuxarıda qeyd olunan texnoloji vasitələrin alqı-satqısı zamanı (i) dövlətin insan hüquqları öhdəliklərinin yoxlanılması, (ii) ictimaiyyətin bu qərarlarda hərtərəfli və mənalı iştirakının müzakirə, konsultasiyalar və s. ilə təmin olunması və (iii) ictimaiyyətin dövri olaraq müvafiq əməliyyatlarının təsdiqi, həyata keçirilməsi və istifadəsinə dair məlumatlandırılması insan hüquqlarının qorunması baxımından daha əlverişli şərait yaradar.[36] Eyni zamanda yazıda daha öncə qeyd edilən, beynəlxalq təşkilat və ekspertlər tərəfindən inkişaf etdirilmiş 'Kommunikasiyaların İzlənməsində İnsan Hüquqlarının Tətbiqinə dair Beynəlxalq Prinsiplər'də də insan hüquqlarına qarşı sui-istifadəyə imkan verəcək texnologiyaların satınalınması prosesində ictimai nəzarətin və məhkəmə nəzarətinin vacibliyi vurğulanır.[37] Başqa sözlə qanunvericilik adıkeçən texnologiyaların gizlincə alınması və istifadəsini hökumət üçün çətinləşdirmədikdə onlardan insanların hüquqları əleyhinə istifadə ehtimalı güclənir.

Azərbaycanda isə yuxarıda adı keçən təminatlara nə hüquqi səviyyədə, nə də təcrübədə rast gəlinir. Əvvəla milli qanunvericilik, daha konkret isə 2001-ci il tarixli "Dövlət Satınalmaları haqqında" qanun satınalmalar prosesi zamanı dövlətin insan hüquqları üzrə öhdəliklərinə baxış və ya izləmə və dinləməyə imkan verəcək texnologiyaların alınması zamanı mümkün məhkəmə nəzarəti ilə bağlı qaydalar müəyyənləşdirmir.[38] Bundan başqa hansı hallarda tenderin açıq və ya qapalı keçiriləcəyinə və müfaviq olaraq qapalı tenderlərlə bağlı məlumatların hansı səviyyədə ictimaiyyətlə bölüşülməsi ilə bağlı dəqiq qaydaların olmaması faktiki olaraq hökumət qurumlarına kritik hesab oluna biləcək məhsulların alqı-satqısı zamanı ölçüsüz mülahizə sərbəstliyi tanıyır. Bundan başqa Azərbaycanda ictimaiyyətin yüksək səviyyəli qərarvermə proseslərinə zəif və ya imitativ cəlbi praktikası da təcrübədə izləmə və dinləmə texnologiyaları ilə bağlı alqı-satqı əməliyyatlarında ictimaiyyətin hərtərəfli və mənalı iştirakını mümkünsüz edir. Vurğulamağa ehtiyac var ki, Azərbaycan hökumətinin adı Pegasus skandalı başda olmaqla bir neçə halda xarici hüquqi şəxslərin istehsalı olan, izləmə və dinləmə və digər müdaxilələrə imkan verən bir neçə viruslu proqramların müştərisi olan hökumətlərin arasında adı hallanıb.[39] Lakin buna baxmayaraq Azərbaycanda müvafiq alqı-satqının hansı qurum

[34] United Nations Human Rights Council, 'Surveillance and human rights Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', (2019), A/HRC/41/35, para 54, https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.ohchr.org%2Fsites%2Fdefault%2Ffiles%2FDocuments%2FIssues%2FOpinion%2FA_HRC_41_35_EN.docx&wdOrigin=BROWSELINK; (A/HRC/41/35)
[35] A/HRC/41/35 – para 54
[36] A/HRC/41/35 – paras 52-4
[37] 13 Prinsip (n18), səhifə 5
[38] E-qanun.az, 'Dövlət Satınalmaları haqqında Azərbaycan Respublikasının qanunu', (2001), 245-IIQ, https://e-qanun.az/framework/1029
[39] Radio Free Europe, 'Azerbaijan Suspected Of Spying On Reporters, Activists By Using Software To Access Phones', (2021), https://www.rferl.org/a/azerbaijan-pegasus-spying-nso/31365076.html; Qurium Media, 'Corruption, Cencorship and a Deep Packet Inspection Vendor', (2018),

tərəfindən, nə zaman və nə məqsədlə aparıldığına dair ictimaiyyətə açıq mənbələrdə məlumat yoxdur. Müxtəlif ölkələrlə Azərbaycan arasında alqı-satqı əməliyyatlarından isə adətən yerli mediaya sızan və ya xarici media orqanları tərəfindən report olunan xəbərlər hesabına xəbər tutmaq mümkün olur.

Tənqidçilərə qarşı kiber hücumlarda hüquqi şəxslərin öhdəliklərinə dair hüquqi təminatların mövcudluğu

Özəl şirkətlərin və ya başqa sözlə biznes qurumlarının hərəkətlərinin insan hüquqlarına təsdiqlənmiş təsirinə dair sübutların artmasının fonunda beynəlxalq təcrübədə hüquqi şəxslərin insan hüquqları ilə bağlı öhdəlikləri də getdikcə daha çox müzakirə edilir. Bu şirkətlərin öhdəliklərinə dair beynəlxalq qanunverici və normayaradıcı nümunələrə məcburiyyət daşımasa da BMT səviyyəsində qəbul edilmiş 'Biznes və İnsan Hüquqlarına dair Bələdçi Prinsiplər' (UNGP – bundan sonra) və elə UNGP-dən ilhamlanan və Aİ məkanında məcburi xarakter daşıyan GDPR-ı nümunə göstərmək olar.[40] Müvafiq olaraq UNGP müəyyən edir ki, şirkətlər insan hüquqlarına təsir edə biləcək əməliyyatlarla bağlı daimi önləyici tədbirlər (*İng*: *human rights due diligence*) həyata keçirməli, bu təsiri ölçməli və risklərə qarşı hazırlıqlı və məsuliyyətli olmalıdır. GDPR isə öz növbəsində insan hüquqlarına, əsasən də fərdi məlumatların qorunması hüququna mənfi təsirin qarşısının alınması üçün bizneslər qarşısında önləyici tədbirlər almaqla bağlı öhdəliklər qoyur. Bu öhdəliklər müvafiq olaraq istifadəçilərin hansı məlumatlarının əldə olunması, istifadəçilərin bununla bağlı məlumatlandırılması, məlumatların hansı müddətdə və necə saxlanılması və silinməsi, üçüncü tərəflərə, o cümlədən, Aİ məkanından kənara ötürülməməsi barədə qaydalar müəyyənləşdirir.[41]

Özəl şirkətlər digər sahələrdə olduğu kimi internet azadlıqlarının qorunmasında da bəzən əhəmiyyətli oyunçu kimi çıxış edə bilirlər. Belə ki, onlar bu landşaftda istifadəçilərin fərdi məlumatların emalçısı kimi hökumət və digər qurumlarla əlaqəyə girir, fərdi məlumatların hökumət qurumları və digərlərinə ötürülməsi və ya müştərilər üçün izləmə və dinləməyə imkan verən texnologiyaların istehsalı, ixrac və ya idxalını həyata keçirə bildikləri üçün avtomatik olaraq öhdəliklərə yiyələnirlər. Təsadüfi deyil ki, hökumətlərə tənqidçiləri izləməyə imkan verən Pegasus proqramının istehsalçısı olan 'NSO Group' şirkəti və ya onunla məhsulundan faydalanaraq insan hüquqlarını pozmaqda ittiham olunan hökumət və qurumlar ən az 5 halda və 4 fərqli yurisdiksiyada insan hüquqlarının pozulmasında roluna görə məhkəməyə verilib.[42]

---

https://www.qurium.org/alerts/azerbaijan/corruption_censorship_and_a_dpi_vendor/; Hackingteam, 'Mapping HackingTeam's Untraceable spyware' (2014), https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware; IPHR report (n5), 92-4

[40] BMT-nin Insan Hüquqları üzrə Ali Komissarlığı, 'Insan Hüquqları və Biznesə dair Bələdçi Prinsiplər: Müdafiə, Hörmət, Bərpa', (2011), https://digitallibrary.un.org/record/720245?ln=en

[41] GDPR.EU, 'A guide to GDPR data privacy requirements', (2023), https://gdpr.eu/data-privacy/

[42] Business and Human Rights Resource Center, 'UK : Activist files lawsuit against NSO Group for invasion of privacy over allegations his phone was hacked with Pegasus spyware', (2022), https://www.business-humanrights.org/en/latest-news/uk-a-prominent-activist-a-launches-lawsuit-against-nso-group-and-bahrain-for-invasion-of-privacy/;
Apple Newsroom, 'Apple sues NSO Group to curb the abuse of state-sponsored spyware', (2021), https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/;
Washington Post, 'Here's a first: Journalists and a U.S. citizen are suing NSO Group', (2022), https://www.washingtonpost.com/politics/2022/12/01/here-first-journalists-us-citizen-are-suing-nso-group/;
İsrail https://www.amnesty.org/en/latest/press-release/2019/05/israel-amnesty-legal-action-stop-nso-group-web-of-surveillance/;

Hökumətlər adətən telekommunikasiya şirkətlərindən istifadəçilərin fərdi məlumatlarının, kommunikasiyalarının onlarla bölüşülməsi üçün xüsusi texnikadan istifadə etməyi tələb edirlər. Bu texnika, yəni hüquq-mühafizə orqanlarına sistemə kənardan birbaşa müdaxiləni (*ing*: *backdoor access, black boxes*) təmin edən texnologiyanın istifadəsi və məlumatların belə tranfserinə qarşı hüquqi təminatların olmaması hüquq-mühafizə orqanlarına insanların şəxsi həyatına müdaxilə üçün ölçüsüz sərbəstlik tanıyır.[43] Nəticədə isə vətəndaşların ifadə azadlığı və fərdi məlumatların təhlükəsizliyi ilə əlaqədar hüquqları təhdid altına düşür.

Azərbaycanda isə biznes qurumlarının müvafiq öhdəlikləri və internet azadlıqlarının pozulmasına qarşı hüquqi təminatların mövcudluğu ilə bağlı çatışmazlıq müşahidə olunur. İlk növbədə Azərbaycanda nə UNGP, nə də GDPR standartlarına uyğun olaraq hüquqi şəxslərdən əməliyyatlarının insan hüquqlarına potensial mənfi təsirlərini ölçmək, riski azaltmaq və qarşısını almaq üçün önləyici tədbirlər almağı tələb edən spesifik qanunvericilik norması yoxdur. Belə olan halda biznes qurumlarının insan hüquqlarına hörmətlə bağlı öhdəlikləri dəqiq müəyyən olunmur və izləmə və dinləməyə imkan verən texnologiyalarının istehsalı, idxalı, ixracı və aidiyyatı xidmətlərin göstərilməsi zamanı pozulan hüquqların bərpası üçün səmərəli fürsətlər tanımır.

Fərdi məlumatların mühafizəsi ilə əlaqəli "Telekommunikasiyalar haqqında" qanunun 38.3-cü maddəsi operatorlar və provayderlərə şəbəkələri vasitəsilə ötürülən məlumatların məxfiliyini təmin etmək öhdəliyi müəyyən edir. Lakin qanunun 33.1.9 və 33.1.9-2 ci maddələri icra hakimiyyəti və hüquq-mühafizə orqanları nümayəndələrinə müvafiq olaraq yerində yoxlamalar aparmağa şərait yaratmaq və sorğulanan məlumatları təqdim etməyi operator və provayderlərin vəzifəsi kimi müəyyən edir. Əlavə olaraq 39-cu maddə isə operator və provayderlərdən əməliyyat-axtarış fəaliyyətini həyata keçirən quruma bu məqsədlə şərait yaratmağı, telekommunkasiya şəbəkəsinə tələb olunan əlavə texniki vasitəni qoşmağı və bu tədbirlərlə bağlı gizliliyi qorumağı tələb edir. Qanunun 17.4-cü maddəsi isə yalnız dövlət nəzarətini həyata keçirən orqanın səlahiyyətlərindən sui-istifadəsi zamanı təkcə inzibati qaydada məhkəməyə müraciət imkanı tanıyır.[44]

Əvvəla bu maddələrin geniş formulasiyası və məlumatların üçüncü tərəflərə ötürülməsi, o cümlədən hüquq-mühafizə orqanlarının bu məlumatların əldə edilməsi, saxlanılması və silinməsi ilə bağlı dəqiq qaydaların müəyyən olunmaması hüquq-mühafizə orqanlarına onların tətbiqi ilə məhdudiyyətsiz imkanlar tanıyır. Həmçinin hüquq-mühafizə orqanlarına telekommunikasiya şirkətlərinin sərəncamında olan potensial olaraq bütün fərdi məlumat və kommunikasiyalara kənardan, birbaşa və tam müdaxilə imkanı verilməsinə və bu hallara qarşı hüquqi təminatların olmaması ayrıseçkilik olmadan bütün vətəndaşların fərdi məlumatlarının fonunda insan hüquqlarına zəruri olmayan və qeyri-proporsional müdaxiləni mümkün edir.

The guardian, 'Israel: Amnesty International engages in legal action to stop NSO Group's web of surveillance', (2019), https://www.theguardian.com/us-news/2020/dec/22/nso-group-spyware-dangerous-say-tech-firms-in-legal-filing;
Business and Human Rights Resources Center, 'Thai activists sue government over abuse of Pegasus software', (2023) https://www.business-humanrights.org/en/latest-news/thai-activists-sue-government-over-abuse-of-pegasus-sypware/;
Access Now, 'Facing the consequences: Access Now welcomes legal action against NSO Group', (2023) https://www.accessnow.org/press-release/legal-action-nso-group/

[43] Human Rights Watch, 'Perils of Back Door Encryption Mandates 'Five Eyes' Nations Should Support, Not Threaten, Digital Security', (2017), https://www.hrw.org/news/2017/06/26/perils-back-door-encryption-mandates

[44] Telekommunikasiyalar haqqında qanun, maddələr 17.4, 33.1.9, 33.1.9-2, 38.3

BMT-nin İfadə Azadlığının Müdafiəsi üzrə Xüsusi Məruzəçisinin 2018-ci il tarixli hesabatında qeyd olunur ki, hökumətlər adətən telekommunikasiya şirkətlərindən məxlifik rejimini (*ing: encyrption)* pozaraq onlara məlumatlara asan müdaxilə imkanı verməyə tələb etsələr də adətən bu yaxşı əsaslandırılmır və hüquq-mühafizə orqanlarının geniş səlahiyyətlərinin fonunda zəruri olmur.[45] Hesabatda qeyd olunur ki, hökumətlərə bütün kommunikasiyalara girişə imkan verən texnologiyalar (arxaqapı girişi, qara qutular və s.) həm insan hüquqlarını təhdid altında qoyduğu üçün, həm də sözügedən məlumatların üçüncü arzuolunmaz tərəflərdən müdafiəsini də çətinləşdirdiyi üçün belə müdaxilə tədbirinə yalnız zəruri halda və legitim məqsədə müvafiq əl atılmalıdır.[46]

Həmçinin AİHM də öz növbəsində insan hüquqlarına istənilən müdaxilənin qanunla müəyyən edilməsini, legitim məqsəd üçün proporsional olmasını və yalnız zəruri edilməsini tələb edir. Bundan başqa *Roman Zaxarov Rusiyaya qarşı* işində məhkəmə qeyd edir ki, hüquq-mühafizə orqanlarının istisnasız bütün kommunikasiyalara birbaşa, məhkəmə nəzarəti olmadan müdaxilə etməsinə şərait yaradan qanunvericilik sui-istifadəyə açıqdır və buna qarşı hüquqi təminlatların olması vacibdir.[47] Bu hüquqi təminatların olmaması isə hüquq-mühafizə orqanları tərəfindən dinləmə və izləmə tədbirlərinin zəruri olmayan və qeyri-proporsional istifadəsinə yol açа və vətəndaşların qorxu və özünü-senzura şəraitində hüquqlarından faydalana bilməməsinə gətirib çıxara bilər.[48]

Təsadüfi deyil ki, Azərbaycanda bir-neçə halda telekommunikasiya şirkətləri vasitəsilə fərdi məlumatlara müdaxilə halları yaşanıb. Belə ki, 2015-ci ildə 'Mütəşəkkil Cinayətkarlıq və Korrupsiya Hesabatı Layihəsi' (OCCRP – bundan sonra) təşkilatının araşdırma nəticələri göstərdi ki, Azərbaycada telekommunikasiya işini həyata keçirən Teliasonera şirkəti hökumətə bütün kommunikasiyalara müdaxilə etmək imkanı verən texnikadan istifadə edib.[49] Digər bir nümunə isə 2019-cu ilin yanvar ayında o zamanlar siyasi məhbus olan Mehman Hüseynovun azadlığa çıxması üçün təşkil edilən aksiyadan sonra kifayət qədər çox sayda və heç də siyasətlə birbaşa əlaqəsi olmayan aksiya iştirakçılarının mobil nömrələrinin ərazidə olması səbəbilə aksiyadan sonra polis bölmələrinə çağırılaraq təzyiq edilməsi ilə bağlı olub.[50] Təcrübədə hüquq-mühafizə orqanları tərəfindən belə sui-istifadə hallarının təsdiqini tapması xüsusilə də qanunvericilikdəki boşluqların fonunda internet azadlıqlarına qarşı böyük təhdidlərdən xəbər verir.

Bundan başqa sonda qeyd etmək olar ki, milli qanunvericilik vətəndaşlara dair məlumatların üçüncü tərəflərə ötürülməsi məsələsində dəqiq qaydalar müəyyən etmədiyi üçün fərdi məlumatlara müdaxilə halından da avtomatik olaraq xəbərsiz qalırlar və bu müdaxilədən şikayət imkanından faktiki olaraq məhrum edilirlər.

---

[45] Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Encryption and Anonymity follow-up report', (2018), paras 13-4 , 49, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

[46] Həmin yerdə

[47] *Roman Zaxarov Rusiyaya qarşı işi*, №. 47143/06, (2015 AIHM), para 270

[48] UN HRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*', (2016), A_HRC_32_38, para 57, https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session32/Documents/A_HRC_32_38_EN.docx;

[49] Organized Crime and Corruption Reporting Project (OCCRP), 'TeliaSonera's behind-the-scenes connection to Azerbaijani president's daughters, (2014), https://www.occrp.org/en/investigations/2531-teliasoneras-behind-the-scenes-connection-to-azerbaijani-presidents-daughters; Telecomix BSRE, 'How Teliasonera Sells to Dictatorships. Uppdrag Granskning : The Black Boxes', (2013), https://vimeo.com/41248885

[50] BBC Azərbaycabca, 'Polisə çağrılanların hekayələri: Filankəs sizin qohumunuzdur, ona deyin, mitinqə getməsin', (2019), https://www.bbc.com/azeri/international-46972971

6. Kiber hücumlar və təhlükəsizliyə dair geniş təsnifatın yoxluğu və vahid qanun təklifi

Son illərdə getdikcə daha çox ölkədə kiber təhlükəsizliyin təmin olunması üçün kiber cinayətkarlıq haqqında qanunlar qəbul olunur. Belə qanunlar kiber cinayətlərin daim yenilənən və qəlizləşən formalarını tərif edir, onların həyata keçirilməsinə görə cinayət məsuliyyəti yaradır, səmərəli istintaq və əməliyyat-axtarış tədbirləri ilə bağlı qaydaları müəyyənləşdirir və kiber təhlükəsizlik sahəsində normalar yaradaraq milli mexanizm rolunu oynayır.

Yuxarıda da qeyd olunduğu kimi Azərbaycanda milli qanunvericilikdə internet azadlıqlarının, o cümlədən fərdi məlumatların mühafizəsi ilə əlaqəli qanunlar olsa da kiber təhlükəsizliyə dair vahid qanuna rast gəlinmir. Vahid qanun kiber təhlükəsizlik sahəsində mütləq uğuru vəd etməsə də qanunvericilikdə bəzi çatışmazlıqları aradan qaldırmaq üçün fürsət kimi istifadə oluna bilər.

Belə ki, əvvəla kiber cinayətlərin həyata keçirildiyi texnologiyalar surətlə inkişaf etdiyi üçün kiber cinayətlərin formaları da fasiləsiz olaraq artır və qəlizləşir. Belə olan halda milli qanunvericilikdə kiber cinayətkarlıqla bağlı anlayışların yer almaması tənqidçilər də daxil olmaqla onlara məruz qalmış şəxslərin hüquqlarının səmərəli müdafiəsini sual altında qoyur. Azərbaycanda yalnız "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" qanunda kiber insident, təhdid və hücum anlayışlarına tərif verir. CM-nin 271-74-cü maddələri isə informasiya sistemləri, kompüterlər və məlumatlara müdaxilə, ələ keçirmə, daxil olma halları ilə sanksiyaları müəyyən edir. Yəni qanunvericiliyin hazırki vəziyyəti Azərbaycanda tənqidçilərə qarşı fişinq, xaker, DDoS hücumları kimi halların cəzalandırılması üçün hüquqi təminatlar yaradır. Bununla belə qanunvericilikdə total internet blokadaları, identifikasiya məlumatlarının oğurluğu, kiber bullinq və zorakılıq kimi Azərbaycanda da kifayət qədər müşahidə edilən internet azadlıqlarına hücumlar və kiber cinayətlərə dair tərif və ya detallı sanksiya müəyyən edən normaya rast gəlinmir. Kiber cinayətkarlıq haqqında qəbul ediləcək qanunsa həm bu, həm də bu yazıda toxunulmamış digər bir çox kiber hücumlara qarşı səmərəli hüquqi müdafiə mexanizmi yarada bilər.

IV. Kiber hücum hallarından qeyri-səmərəli araşdırmalar

Kiber təhlükəsizliyin təmin olunması üçün hüquqi, siyasi və digər elementləri ehtiva edən kompleks tədbirlərin yoxluğu həm dövlət, həm də vətəndaşları texnologiyanın inkişaf etdiyi dövrdə asan hədəfə çevirə, həssas məlumatların arzuolunmaz oyunçular tərəfindən oğurlanmasına gətirə bilər. Öncədən də qeyd olunduğu kimi dövlətlərin insan hüquqları ilə bağlı öhdəlikləri internet azadlıqlarına da şamil olunur. Bu kontekstdə dövlətlər müvafiq olaraq bu hüquqlardan istifadəyə hörmətlə yanaşmalı, ondan tam yararlanmaq üçün şərtləri təmin etməli və bu hüquqlara qarşı müdaxilələrin qarşısını almalıdır. Sonuncu öhdəliyin kiber hücumlar kontekstində mənası budur ki, dövlətlər tənqidçilərə yönəlik kiber hücumlarda pozuntunun aradan qaldırılması üçün səmərəli araşdırmalar həyata keçirməli və təqsirli şəxsləri məsuliyyətə cəlb etməlidir. Müvafiq olaraq AİHM də müxtəlif qərarlarda, o cümlədən *Xədicə İsmayılova Azərbaycana qarşı* işində ərizəçinin şəxsi həyatına müdaxilə halının səlahiyyətli orqanlar tərəfindən səmərəli şəkildə araşdırılmamasını pozuntu kimi tanıyıb.[51] Məhkəmə qeyd edir ki, səmərəli hesab olunmaq üçün istintaq işin hallarını müəyyən etməyə, təqsirli şəxsləri müəyyənləşdirməyə və cəzalandırmağa qadir olmalıdır.[52]

[51] *Xədicə İsmayılova Azərbaycana qarşı işi,* №*65286/13* (2019 AİHM), paras. 118, 131-2
[52] Həmin yerdə

Azərbaycanda internet istifadəçilərinə qarşı kiber hücumları dəqiq definisiya edən vahid qanun olmasa da əksər kiber hücumların cinayət məsuliyyətinə cəlb olunması üçün CM-nin 271–74-cü maddələri mövcud olması hüquq-mühafizə orqanlarına müvafiq araşdırmalar aparmağa hüquqi fürsət tanıyır.[53]

Bundan başqa kiber hücumlar sürətlə inkişaf edən informasiya kompüter texnologiyalarının vasitəsilə həyata keçirildiyi üçün onlara dair araşdırmalar aparmaq hər keçən daha da qəlizləşir və xüsusi bacarıq və səlahiyyətlərə malik qurumların mövcudluğunu tələb edir. Bu mənada Azərbaycanda Rəqəmsal İnkişaf və Nəqliyyat Nazirliyinin nəzdində 'Elektron Təhlükəsizlik Xidməti' və birbaşa prezidentə tabe olan 'Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti' fəaliyyət göstərir. Xidmətlərin əsasnamələrindən məlum olur ki, hər iki qurum kiber təhlükəsizlik sahəsində məlumat toplanılması və ictimaiyyətin məlumatlandırılması vəzifələri daşısa da, XRİTDX həm də kiber insidentlərin araşdırılmasında aidiyyatı orqanlara yardım səlahiyyətinə malikdir.[54] Eyni zamanda "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə qanuna əsasən DTX (Milli Təhlükəsizlik Nazirliyinin hüquqi varisi imi) kiber cinayətkarlıq hallarında səmərəli istintaqa yardım məqsədilə 7/24 fəaliyyət göstərən qurum kimi təyin olunur.[55] Bu isə DTX-ya Konvensiya tərəfdaşlarının mərkəzi məlumat mübadiləsi sisteminə daimi keçid verərək səmərəli istintaq aparma fürsəti yaradır.

Yəni ümumi mənzərədə Azərbaycanda təkmil halda olmasa da kiber cinayətlərə dair əsas aspektləri əhatə edən qanunvericilik və ixtisaslı qurumların timsalında səmərəli istintaqa imkan verən şərtlərin mövcudluğunu var saymaq olar. Bununla belə, növbəti paraqraflarda müzakirə olunduğu kimi, bu günə qədər tənqidçilərə qarşı törədilmiş kiber hücumların heç birində səmərəli istintaq aparılmaması faktı yuxarıda imkanların səmərəliliyini sual altında qoyur. Bununla belə qeyd etmək lazımdır ki, Azərbaycan "Kibercinayətkarlıq haqqında" Budapeşt Konvensiyasının ölkələrə öz ərazilərindən kənardan planlanmış və ya icra edilən kiber cinayətlərlə bağlı səmərəli araşdırma aparmaq üçün imkanlar tanıyan və öhdəliklər müəyyən edən ikinci əlavə protokoluna qoşulmayıb.[56]

Daha öncə qeyd edildiyi kimi 2017-ci ildən etibarən ən az 46 halda hökumət tənqidçilərinin kiber hücumlara məruz qalması faktı zərərçəkənlərin özləri tərəfindən və ya mediada işıqlandırılıb.[57] Azərbaycanda CPM-in 46.2-ci və 207.1.1-ci maddələrinə əsasən Prokurorluq orqanları hüquq pozuntuları barədə mediada yayılmış informasiya əsasında cinayət işi açmaq səlahiyyətinə malik olsalar da yuxarıda qeyd olunan insidentlərin heç birində oxşar hala rastlanmayıb.[58]

Hətta bəzi hallarda zərərçəkən şəxslərin şikayətlərinə baxmayaraq aidiyyatı qurumlar araşdırma aparmaqdan boyun qaçırıblar. Misal üçün ictimai fəal Bəxtiyar Hacıyev, 2023-cü

[53] Cinayət Məcəlləsi, maddələr 271-4
[54] Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi üzrə Dövlət Xidməti, 'Kiber Təhlükəsizlik', (2023), https://scis.gov.az/az/pages/view/cyber;
Rəqəmsal İnkişaf və Nəqliyyat Nazirliyinin Elektron Təhlükəsizlik Xidməti, 'Əsasnamə', (2023), https://cert.az/az/qanunvericilik/esasname1
[55] E-qanun.az, 'Kibercinayətkarlıq haqqında Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu', (2009), № 874-IIIQ, Azərbaycan Respublikasının "Kibercinayətkarlıq haqqında" Konvensiyanın 35-ci maddəsinin 1-ci bəndi üzrə BƏYANATI, https://e-qanun.az/framework/18619
[56] Council of Europe Committee of Ministers, 'Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence', (2021), CETS No. 224, https://www.coe.int/en/web/cybercrime/second-additional-protocol
[57] Ətraflı məlumat üçün bax: 1 Nömrəli qoşma
[58] Cinayət Prosessual Məcəlləsi, maddələr 46.2, 207.1.1

ilin Martın 9-da onlayn məkanda bir bloger tərəfindən təhdid olunduğunu, adından şəxsi yazışmalar yayıldığını, yəni kiber zorakılığa məruz qaldığını bildirsə də, nə DİN, nə Baş Prokurorluq, nə də yerli məhkəmələr bu hallara dair araşdırma aparmağa razı olmayıb.[59] 2021-ci ilin mart ayında insan hüquq müdafiəçiləri Nərmin Şahmarzadənin onlayn profilləri xaker hücumu ilə ələ keçirildikdən sonra onun şəxsi yazışmaları internetdə yayımlanıb.[60] Aktivist yazışmada adı keçən digər fəal Bəxtiyar Hacıyevlə birlikdə hüquq-mühafizə orqanlarının bu hücumların arxasında olduğuna inandığını açıqlayıb. Bundan sonra hadisənin araşdırılacağına dair rəsmi açıqlama verilsə də istintaq tədbirləri nəticəsiz olaraq yekunlaşıb.[61] Gender aktivisti Gulnara Mehdiyevanın onlayn hesabları 2020-ci il martın 8-də keçiriləcək feminist aksiyadan öncə ələ keçirilib. Nəticədə aktivistin şəxsi yazışmaları sosial şəbəkələrdə yayımlanıb. Aktivist bununla bağlı DİN-ə müraciət etsə də onun şikayəti üzrə cinayət işinin açılmayacağı cavabını alıb.[62]

Bundan başqa vətəndaş cəmiyyəti fəalları Anar Məmmədli və Akif Qurbanov Pegasus proqramı ilə izləndikləri ilə bağlı Baş Prokurorluğa şikayət ünvanlasalar da onlardan araşdırmalarla bağlı izahatı DTX alıb.[63] Fəallar Prokurorluğun araşdırma aparmamasını tənqid edib, DTX-nın aparacağı araşdırma ilə bağlı isə inamsızlıqlarını dilə gətiriblər. Qeyd etmək lazımdır ki, fəallar 2021-ci ilin sonlarında şikayət təqdim etsələr də bu yazı yayımlandığı tarixə qədər (İyun 2023) istintaq nəticələrinə dair məlumat ictimaiyyətlə paylaşılmayıb.

V. Kiberhücumların siyasi əhəmiyyəti

Daha öncə də qeyd olunduğu kimi Azərbaycanda xüsusilə də 2017-ci ildən etibarən tənqidçilərin internet azadlıqlarına yönələn kiber hücumların artan xətti müşahidə olunmaqdadır. Əksər hallarda mediada insan hüquq müdafiəçiləri, demokratiya aktivistləri, siyasətçilər, jurnalistlər, internet mediaları və digər tənqidçilərə aid məlumat və səhifələrin müxtəlif kiber hücumlar vasitəsilə oğurlanması, paylaşılması, silinməsi, şantaj predmeti kimi istifadə olunması hallarına rast gəlinib. Araşdırma nəticələrimiz göstərir ki, təkcə 2017-ci ildən bu günə qədər ən az 46 belə halda tənqidçilər kiber hücumlardan zərər çəkiblər.[64] Bəzi önə çıxan məqamları vurğulamaq olar;

Bu hücumların arasında ən böyük yeri tənqidçi fərdlərə qarşı fişinq hücumları tutur. Belə ki, müxtəlif hallarda insan hüquq müdafiəçiləri, vətəndaş cəmiyyəti təmsilçiləri və jurnalistlər naməlum mənbələrdən qrantlar, ödənişlər və ya digər peşə fəaliyyətləri ilə əlaqədar məzmunlu onlayn məktublar alıblar. Bu məktublarda göndərilən faylların fişinq hücumu üçün tərtib olunması bəzən oğurlanan məlumatların, bəzən də aparılan texnoloji araşdırmaların sayəsində

[59] Azadlıq Radiosu, 'Məhkəmə Bəxtiyar Hacıyevin şikayətinə baxmaqdan imtina etdi', (2022), https://www.azadliq.org/a/baxtiyar-haciyev/31811179.html
[60] BBC Azərbaycanca, 'Bəxtiyar Hacıyev və Nərmin Şahmarzadə kiberhücumlarda Azərbaycan hakimiyyətini günahlandırırlar', (2021), https://www.bbc.com/azeri/azerbaijan-56435830
[61] Turan IA, 'İctimai fəalların şəxsi həyatına müdaxilə ilə bağlı hüquq mühafizə orqanları araşdırma aparır', (2021), https://www.turan.az/ext/news/2021/3/free/Social/az/2190.htm
[62] Front Line Defeders, 'Azerbaijan: Smear campaign against woman human rights defender Gulnara Mehdiyeva', (2021), 'azerbaijan_-_ua_-_gulnara_mehdiyeva_-_5_mar_2021_en.pdf (frontlinedefenders.org)
[63] MeydanTV, 'Pegasusla dinlənildiyi güman edilən ictimai şəxslərdən DTX izahat alır', (2022), https://d9mc3ts4czbpr.cloudfront.net/az/article/dtx-pegasusla-dinlenildiyi-guman-edilen-ictimai-sexslerden-izahat-alir/
[64] Ətraflı məlumat üçün bax: 1 Nömrəli qoşma

bəlli olub. Hətta araşdırmalar bir neçə halda hücumların arxasında duran şəxs və mənbələrin DİN və DTX və RİNN-ə bağlı olduğuna dair əsaslı nəticələrə gəlib.[65]

Digər bir geniş yayılmış ənənə isə xaker hücumları ilə bağlıdır. Ən az 31 halda tənqidçi fərdlər və təşkilatlara qarşı xaker hücumları qeydə alınıb. Belə ki, facebook, gmail və digər onlayn platformalarda ikili-doğrulama sistemində mobil nömrədən istifadə edən şəxslərə bəzən müraciət etmədikləri halda şifrə yenilənməsi istəyi gəlib, ardınca isə SMS sisteminə müdaxilə nəticəsində onların və onlara bağlı media qurumlarının onlayn hesabları ələ keçirilib, şəxsi və ya təşkilati məlumatlar oğurlanıb, silinib, bəzən də icazəsiz olaraq paylaşılıb.[66] Belə işlərin bir neçəsində müdaxilə heç SMS-ə ehtiyac olmadan belə gerçəkləşib. Bu isə ümumiyyətlə cihazın başqa üsullarla, o cümlədən Pegasus proqramı vasitəsilə yolxudurulmasına dair şübhələr yaradıb. İnternet medialara edilən hücumlarsa xüsusilə hökumətə dair tənqidi və ya korrupsiya ittihamlarına dair materiallar dərc edilməsindən sonraya təsadüf etdiyi üçün diqqət çəkib.

2021-ci ildə isə Pegasus skandalı internet azadlıqlarına olan hədələrin ən böyüyü kimi ilə damğasını vurub. Belə ki, 'Forbidden Stories' və 'Amnesty International' təşkilatlarının birgə araşdırmaları nəticəsində məlum olub ki, İsraildə qərarlaşan 'NSO Group' şirkətinin istehsalı olan Pegasus programı vasitəsilə, içində Azərbaycan hökumətinin də iddia olunduğu onlarla hökumət sahiblərinin aralarında tənqidçi, müxalif və digər şəxslərin də olduğu 50000-dən artıq mobil cihazı viruslu proqramla yoluxduraraq izləyiblər.[67] OCCRP-ın paylaşdığı siyahıya və iddialara əsasən Azərbaycanda da 80-dən çox şəxsin cihazlarına müdaxilə edilib.[68] Xüsusilə qeyd etmək lazımdır ki, növünün pis mənada ən yaxşısı hesab olunan proqram xüsusilə də tənqidçi qurbanları çıxılmaz vəziyyətdə qoyub, bəzilərini isə hətta texnoloji vasitələrdən böyük ölçüdə imtina etməyə məcbur edib.[69]

İnternet medialarına qarşı DDoS hücumları da geniş istifadə olunan metodlar arasında olub. Belə ki, 2017-ci ildən etibarən ən az 11 halda internet mediaları onların vebsaytlarına çatımlılığı bloklayan hücumlara məruz qalıblar. Azərbaycanda kiber hücumlar arasında yuxarıda qeyd edilən 3 növə ən çox rastlansa da tənqidçilər digər növ hücumlara, o cümlədən kiber zorakılığa məruz qalıblar. Belə ki, bir neçə halda kiber hücumlar nəticəsində ələ keçirilmiş şəxsi yazışmalar və digər məlumatlar vasitəsilə tənqidçilər şantaj olunub, materiallar internet məkanında yayılıb və ya onlara qarşı koordinasiya olunmuş onlayn qısnama tədbirləri həyata keçirilib.[70]

---

[65] Qurium Media Foundation, 'Azerbaijan and the Fineproxy Diy Ddos Service (Region40 / Qualitynetwork)', (2018), https://www.qurium.org/alerts/azerbaijan/azerbaijan-and-the-region40-ddos-service/;
Qurium Media Foundation, 'Finding Man; the Phisher of Journalists in Azerbaijan', (2020), https://www.qurium.org/alerts/azerbaijan/finding-man-the-phisher-of-journalists-in-azerbaijan/;
Azerbaijan Internet Watch (AIW), 'targeted harassment via telegram channels and hacked Facebook accounts' (2021), https://www.az-netwatch.org/news/targeted-harassment-via-telegram-channels/;
PHR-AIW, 'Pulling the plug: How Azerbaijan's government combines technology and fear to control the internet', (2021), p 32, https://www.iphronline.org/wp-content/uploads/2021/09/Pulling-the-Plug_report_updated_compressed-1.pdf;
AIW, 'Another phishing attempt', (2020), https://www.az-netwatch.org/news/another-phishing-attempt/ ;
Ətraflı məlumat üçün bax: 1 nömrəli qoşma
[66] IPHR report (n5), səhifələr 92-4
[67] OCCRP, 'Pegasus Project', (2021), https://www.occrp.org/en/the-pegasus-project/
[68] OCCRP, 'Pegasus Project: Navigate by Country', (2021), https://cdn.occrp.org/projects/project-p/#/
[69] Council of Europe Committee of Ministers, 'Communication from the applicant (07/06/2022) in the case of Khadija Ismayilova v. Azerbaijan (Application No. 65286/13)', (2022), paras 22-30, https://hudoc.exec.coe.int/eng?i=DH-DD(2022)615E
[70] IPHR Report (n5), pages 92-94

Bütün bu hücumların təhlili zamanı aşağıdakı nəticələrə gəlmək olar;

(i) Hücumların ortaq cəhəti onların Azərbaycanda vətəndaş cəmiyyəti və mediada yer alan, insan hüquqları və demokratik dəyərlərin qorunması ilə bağlı fəaliyyət göstərən şəxsləri hədəf almasıdır.
(ii) Bu hücumların həyata keçirilməsində vahid tarixi qanunauyğunluq müşahidə edilməsə də, kifayət qədər çox sayda hücumun xüsusilə də böyük aksiyalardan əvvəl və sonraya, hökuməti tənqid edən media araşdırmaları və xəbərlərin yayılması əsnası və sonrasına təsadüf etməsi də hücumların siyasi məqsədinə işarə verir
(iii) Hücumların sayı və davamlılığı, istifadə olunan üsul, vasitə və nəticələrin oxşarlığı onların təsadüfən həyata keçirilmiş, izolyasiya halında dəyərləndirilə biləcək insidentlər yox koordinasiyalı şəkildə planlanan və həyata keçiridiyini və sistematik bir qanunauyğunluğa malik olduğunu deməyə əsas verir

Həm hədəf alınan şəxslərin ictimai-siyasi kimlikləri, həm də hücumun predmetini təşkil edən məlumatların ictimai-siyasi cəhətdən həssas, tənqidi məlumatlar olması bu kiber hücumların tənqidçilərin insan hüquqları fəaliyyəti ilə bağlı olduğunu deməyə əsas verir. Bu arqumenti daha da gücləndirən digər bir məsələ isə bundan öncəki bölmədə müzakirə olunduğu kimi əksər hallarda tənqidçilərə yönəlmiş kiber hücumlara münasibətdə hətta hökumətin bu hücunların arxasında durduğuna inanmağa əsas verən araşdırma nəticələrinə baxmayaraq rəsmi qurumların laqeyd münasibəti və ya heç bir halda nəticə verməmiş istintaq tədbirləri və yekun görüntüdə cəzasızlıq mühitidir. Yuxarıda sadalanan amillər kiber hücumların Azərbaycanda hökumətin müxalif və tənqidi səsləri susdurmaq üçün istifadə etdiyi növbəti, kompleks və təəssüf ki, səmərəli metod olduğunu deməyə əsas verir.

VI. Yekun

Sonda qeyd etmək olar ki, Azərbaycanda, xüsusilə də, tənqidçilərin internet azadlıqlarına qarşı kiber hücumların son illərdə artdığı müşahidə olunur. Tənqidçilərin cihazlarına və məlumatlarına onlayn müdaxilələr nəticəsində onların fərdi məlumatları ələ keçirilir, silinir, paylaşılır, peşəkar fəaliyyətləri təhdid altına düşür. Milli qanunvericilikdə internet azadlıqlarına yönəlmiş kiber hücumlara qarşı müəyyən hüquqi təminatlar olsa da ümumi mənzərədə qanunvericilik səmərəli müdafiə üçün yetərli deyil. Müxtəlif qanun və normalar hüquq-mühafizə orqanlarına insanların fərdi məlumatlarına müdaxilə üçün ölçüsüz imkanlar tanıyır, izləmə və dinləməyə imkan verən texnologiyaların satınalınması ilə bağlı şəffaflıq təmin olunmur, kiber cinayətlərin bütün növlərini əhatə edən təkmil qanunvericilik normasına rast gəlinmir. Eyni zamanda kiber hücumlarla bağlı informasiyaların mediada geniş yayımlanmasına və zərərçəkən şəxslərin şikayətlərinə və rəsmi qurumların bu şikayəti araşdırması üçün müəyyən imkanlara baxmayaraq təcrübədə bu hallara dair səmərə vermiş istintaq tədbirləri müşahidə olunmur, hətta bəzi hallarda araşdırma aparmaqdan imtina edilir. Kiber hücumların təhlili isə onların sayı və intensivliyi, hədəf alınan şəxs və təşkilatların kimliyi, məzmunların xarakteri, üsul və vasitələr və ələ keçirilmiş məlumatlarla davranış kimi göstəricilərin fonunda hücumların sistematik xarakter daşıdığını, tənqidçiləri susdurmaq üçün siyasi motivlə həyata keçirildiyini deməyə əsas verir. Sonda qeyd etmək vacibdir ki, qanunvericilik və təcrübədə qarşılaşılan çatışmazlıqların təhlili problemin həllinin təkcə hüquqi tədbirlər yox həm də siyasi iradə gərəkdirdiyini göstərir.

Qoşma 1. Azərbaycanda tənqidçilərə qarşı kiber hücumların 2017-2023-cü illər üzrə qeydə alınan halları

No	Tarix	Şəxs və ya Təşkilatın adı	Zərərçəkənin profili	Hücumun növü	Mənbə	Hücumla əlaqələndirilən qurum
1	2017	Abzas media	Internet mediası	Ddos hücumları	https://www.qurium.org/alerts/news-media-websites-attacked-from-governmental-infrastructure-in-azerbaijan/	Xarici İşlər Nazirliyi, Nazirlər Kabineti, Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi
2	2018	Azadliq.info	Internet mediası	Ddos hücumları	https://www.qurium.org/alerts/azerbaijan/sandvine-and-internet-blocking-in-azerbaijan/	
3	2018	Gunun sesi.info	Internet mediası	Ddos hücumları	https://www.qurium.org/alerts/azerbaijan/azerbaijan-and-the-region40-ddos-service/	Dövlət Təhlükəsizliyi Xidməti
4	2018	Azadliq.info	İnternet media	Ddos hücumları	https://www.qurium.org/alerts/azerbaijan/azerbaijan-and-the-region40-ddos-service/	Dövlət Təhlükəsizliyi Xidməti
5	2019	Azadliq.info	İnternet media	Ddos hücumları	https://www.qurium.org/alerts/azerbaijan/azerbaijan-media-websites-from-azerbaijan-under-ddos/	
6	2019	Gunun sesi.info	Internet mediası	Ddos hücumları	https://www.qurium.org/alerts/azerbaijan/azerbaijan-media-websites-from-azerbaijan-under-ddos/	
7	2019	Abzas media	Internet mediası	Ddos hücumları	https://www.qurium.org/alerts/azerbaijan/azerbaijan-media-websites-from-azerbaijan-under-ddos/	
8	2019	Timetv	Internet mediası	Ddos hücumları	https://www.qurium.org/alerts/azerbaijan/finding-man-the-phisher-of-journalists-in-azerbaijan/	Daxili İşlər Nazirliyi
9	2019	24saat.org	Internet mediası	Ddos hücumları	https://www.qurium.org/alerts/azerbaijan/azerbaijan-media-websites-from-azerbaijan-under-ddos/	
10	2020	Turan	Internet mediası	Ddos hücumları	https://www.az-netwatch.org/news/news-agency-website-ddosed-updated/	

11	2020	Meydan TV	Internet mediası	Ddos hücumları	https://www.az-netwatch.org/news/news-platform-targeted-online/138	
12	2018	Meydan TV	Internet mediası	Xaker hücumları	https://www.opendemocracy.net/en/odr/azerbaijans-authoritarianism-goes-digital/	
13	2018	Ali Karimli	Müxalif siyasətçi	Xaker hücumları	https://www.opendemocracy.net/en/odr/azerbaijans-authoritarianism-goes-digital/	
14	2018	Jamil Hasanli	Müxalif siyasətçi	Xaker hücumları	https://www.opendemocracy.net/en/odr/azerbaijans-authoritarianism-goes-digital/	
15	2019	Gultakin Hajibayli	Müxalif siyasətçi	Xaker hücumları	https://jam-news.net/baku-wiretapping-scandal-audio-recordings-of-conversations-of-diplomats-with-opposition-figure-broadcast-on-tv/	
16	2020	Meydan TV	Internet mediası	Xaker hücumları	https://www.az-netwatch.org/news/news-platform-targeted-online/138	
17	2020	basta.info	Internet mediası	Xaker hücumları	https://www.az-netwatch.org/news/facebook-page-affiliated-with-opposition-hackedagain/	
18	2020	Müsavat Partiyasının üzvləri	Müxalif Siyasi Partiya	Xaker hücumları	https://www.az-netwatch.org/news/opposition-party-social-media-accounts-hacked/	
19	2020	Rustam Ismayilbayli	Aktivist	Xaker hücumları	https://www.az-netwatch.org/news/targeted-harassment-via-telegram-channels/; https://www.iphronline.org/wp-content/uploads/2021/09/Pulling-the-Plug_report_updated_compressed-1.pdf	Dövlət Təhlükəsizliyi Xidməti
20	2020	Gultakin Hajibayli	Müxalif siyasətçi	Xaker hücumları	https://www.az-netwatch.org/news/opposition-activist-instagram-account-hacked/	
21	2021	Vafa Nagi	İnsan Hüquq Müdafiəçisi	Xaker hücumları	https://www.az-netwatch.org/news/targeted-harassment-via-telegram-channels/	

22	2021	Fatima Movlamli	Jurnalist	Xaker hücumları	https://www.az-netwatch.org/news/targeted-harassment-via-telegram-channels/	
23	2021	Narmin Shahmarzada and Bakhtiyar Hajiyev	İnsan Hüquq Müdafiəçisi	Xaker hücumları	https://www.turan.az/ext/news/2021/3/free/Social/az/2190.htm	
24	2021	Gulnara Mehdiyeva	İnsan Hüquq Müdafiəçisi	Xaker hücumları	https://www.az-netwatch.org/news/activists-personal-messages-leaked-after-hacking/	
25	2023	Red Line Channel	Internet mediası	Xaker hücumları	https://www.az-netwatch.org/news/news-platforms-facebook-page-hacked-year-worth-of-content-deleted/	
26	2020	Anews.az	Internet mediası	Xaker hücumları	https://www.az-netwatch.org/news/several-facebook-pages-compromised/	
27	2020	Abzas media	Internet mediası	Xaker hücumları	https://www.az-netwatch.org/news/independent-news-site-hacked/	
28	2020	Argument.az	Internet mediası	Xaker hücumları	https://www.az-netwatch.org/news/argument-az-facebook-page-hacked/	
29	2020	Intigam Aliyev	İnsan Hüquq Müdafiəçisi	Xaker hücumları	https://www.az-netwatch.org/news/hacking-alert-activists-and-journalists-targeted-online-ongoing/	
30	2020	D18 Movement	Siyasi hərəkat	Xaker hücumları	https://www.az-netwatch.org/news/hacking-alert-activists-and-journalists-targeted-online-ongoing/	
31	2020	Aysel Umudova	Jurnalist	Xaker hücumları	https://www.az-netwatch.org/news/hacking-alert-activists-and-journalists-targeted-online-ongoing/	
32	2020	Fatima Movlamli	Jurnalist	Xaker hücumları	https://www.az-netwatch.org/news/hacking-alert-activists-and-journalists-targeted-online-ongoing/	
33	2020	Rustam	Aktivist	Xaker hücumları	https://www.az-netwatch.org/news/hacking-	

		Ismayilbayli			alert-activists-and-journalists-targeted-online-ongoing/	
34	2020	Mehman Huseynov	Blogger	Xaker hücumları	https://www.az-netwatch.org/news/how-to-silence-corruption-the-tale-of-one-citizen-journalist-and-a-government-that-does-not-want-people-to-know-the-truth/	
35	2018	Aziz Karimov	Jurnalist	Xaker hücumu (SMS müdaxilə)	https://www.iphronline.org/wp-content/uploads/2021/09/Pulling-the-Plug_report_updated_compressed-1.pdf	
36	2018	Radio Free Liberty	Internet mediası	Xaker hücumu (SMS müdaxilə)	https://www.iphronline.org/wp-content/uploads/2021/09/Pulling-the-Plug_report_updated_compressed-1.pdf	Təhsil Nazirliyi
37	2020	Gulnara Mehdiyeva	İnsan Hüquq Müdafiəçisi	Xaker hücumu (SMS müdaxilə)	https://www.az-netwatch.org/news/activists-personal-messages-leaked-after-hacking/	
38	2020	Nefest LGBT	Vətəndaş cəmiyyəti təşkilatı	Xaker hücumu (SMS müdaxilə)	https://www.az-netwatch.org/news/coordinated-digital-attacks-against-feminist-movement-members-and-lgbt-rights-activists/	
39	2020	Minority Magazine	Vətəndaş cəmiyyəti təşkilatı	Xaker hücumu (SMS müdaxilə)	https://www.az-netwatch.org/news/coordinated-digital-attacks-against-feminist-movement-members-and-lgbt-rights-activists/	
40	2021	Toplum TV	İnsan Hüquq Müdafiəçisi	Xaker hücumu (SMS müdaxilə)	https://www.az-netwatch.org/news/toplum-tv-facebook-page-hacked-via-sms-interception/	
41	2022	Toplum TV	Internet mediası	Xaker hücumu (SMS	https://www.az-netwatch.org/news/online-news-platform-hacked-content-and-followers-removed/	

				müdaxilə)		
42	2020	Sancaq TV	Internet mediası	Xaker hücumu cəhdi	https://www.az-netwatch.org/news/how-to-silence-corruption-the-tale-of-one-citizen-journalist-and-a-government-that-does-not-want-people-to-know-the-truth/	
43	2020	Intigam Aliyev	İnsan Hüquq Müdafiəçisi	Fişinq hücumu	https://www.az-netwatch.org/news/another-phishing-attempt/	Daxili İşlər Nazirliyi
44	2020	Vətəndaş cəmiyyəti fəalları	Vətəndaş cəmiyyəti fəalları	Fişinq hücumu	https://www.iphronline.org/wp-content/uploads/2021/09/Pulling-the-Plug_report_updated_compressed-1.pdf	Daxili İşlər Nazirliyi
45	2022	Abulfaz Gurbanli	İnsan Hüquq Müdafiəçisi	Fişinq hücumu	https://www.az-netwatch.org/news/deliberate-targeting-in-pro-government-media-leads-to-targeted-attacks-online-the-case-of-abulfaz-gurbanli/	
46	2023	Bakhtiyar Hajiyev	İnsan Hüquq Müdafiəçisi	Kiber zorakılıq	https://www.azadliq.org/a/baxtiyar-haciyev/31811179.html	