YENİ DÖVLƏT MODELİ: HAKERDÖVLƏTDƏN YENİ TƏHLÜKƏSİZLİK QAYĞILARINA

Əziz Əlibəyli

Sosial Tədqiqatlar Mərkəzinin Media və Kommunikasiya Departamentinin rəhbəri
e-mail: azizalibeyli@gmail. com

Xülasə

Məqalədə kiber dünyanın yeni keyfiyyətlərinə toxunulur, onun əhatə etdiyi yeni detallar aşkar edilir. Kiber dünyanın yaranması, inkişafı və hazırkı vəziyyəti izah edilir. Müasir dünyamızda artıq dövlətlərin hakerliyi anlayışı izah edilir. Eyni zamanda formalaşan yeni dünya nizamı kontekstində kiber hücumlar milli təhlükəsizliyin aspekti kimi, informasiya müharibəsinin tərkib hissəsi kimi nəzərdən keçirilir.

Məqalədə kəmiyyət və keyfiyyət analizi, müqayisə metodu və tarixi ardıcıllıq metodlarından istifadə edilib.

Açar sözlər: *Kibercinayətkarlıq, kiberterror, kiberdövlət, sosial şəbəkələr, informasiya müharibəsi*

Giriş

Kiberterrorizm kibermәkanda hücumlar edәrәk hökumәtlәrә vә ya mülki şәxslәrә zәrәr vuran şәxslәr vә ya qruplar tәrәfindәn hәyata keçirilәn tәhlükәli fәaliyyәt olaraq son illәrdә çox mәşhurlaşıb. Bununla yanaşı günümüzdә kiberhücumların dövlәtlәr arasında baş verməsi müşahidә olunur. Odur ki, artıq bir dövlәtin digәr dövlәtlәrә qarşı kiberhücumlar tәşkil etdiyi iddia oluna bilәr. Bu cür iddialar çox vaxt beynәlxalq münasibәtlәr vә tәhlükәsizlik mәsәlәlәri ilә bağlı mürәkkәb vә hәssas mәsәlәlәri gündәmә gәtirir.

Düzdür, son dünya nizamını hәlә dә koordinasiya edәn BMT – "Potsdam" sistemi aktual olsa da, beynәlxalq hüququn tәtbiq sәrhәdlәri vә tәlәblәri dәyişәcәk kimi görünür. Ona görә dә beynәlxalq müqavilәlәrdә keçәrli olan "belә hallar beynәlxalq hüquq vә diplomatik danışıqlar yolu ilә hәll edilmәlidir" fikrinin özü dә ciddi mübahisә predmetidir.

Kibertәhlükәsizlik mühüm mәsәlәdir: hökumәtlәr vә әlaqәdar qurumlar kiberhücumlardan ehtiyat tәdbirlәri görmәyә vә müdafiәni tәmin etmәyә çalışsalar da, kibertәhlükәsizlik kiberhücumların aşkarlanması, qarşısının alınması vә hücumdan sonrakı bәrpanın tәmin edilmәsi üçün texnoloji tәdbirlәr, siyasәt vә әmәkdaşlıq tәlәb edәn bir meqa-prosesdir.

Maraqlıdır ki, bir müddәt әvvәl bu tipli qlobal cinayәtlәri müxtәlif formada tәsrifləndirәn BMT vә digәr hüquq-şәrh qurumları ilk dәfә ötәn әsrin 90-cı illәrindәn ədəbiyyata "kompüter terrorizmi" anlayışını gәtirdilәr. Amma göründüyü kimi, kiberterror artıq hansısa fläş-kartda, proqram tәminatına virus bulaşdırmaq mәrhәlәsindәn çoxdan keçәrәk beynәlxalq cinayәt hüququnda "cinayәtkar kiber dövlәt" anlayışına qәdәr inkişaf etdi.

(Burda "dövlәt" anlayışı tәmsilçi şәxslәrin analogiyası kimi işlәnir. Beynәlxalq hüquqda mәsuliyyәt dövlәtlәrә aid deyil, şәxslәrә, icraçılara aiddir – müәl.)

2000-ci ilin әvvәllәrindә şәxslәrin vә ya qrupların kütlәvi şәkildә hәdәflәrә yeni terror hücumu növündәn istifadә etmәsi halına rast gәlinmәyә başladı.

İlk dәfә ABŞ-ın DİSA şirkәti 1995-ci ildә Pentaqonun elektron sisteminә haker hücumlarının sınağını tәşkil etmiş, nәticә demәk olar ki, dünyanın ən güclü dövlәtinin tәhlükәsizlik üzrә cavabdeh şәxlәrini şoka salmışdı.

ABŞ Müdafiә Nazirliyinin 8900-dәn çox kompüterinin 88 faizi әlә keçirilmiş, proqram tәminatına müdaxilә edilmişdir.

Bu, hadisә göstәrdi ki, ikinci minilliyin tәhlükәsizlik standartları mütlәq dәyişikliyә uğrayacaq vә biz yeni yanaşmalarla üz-üzә qalacağıq.

Daha sonra "The Citibank Hack (1995)" hadisәsi dünya bank sistemi üçün zәlzәlә effekti yaratdı. Vladimir Levin "Citibank"ın telefon vә kompüter sistemlәrini sındıraraq 10,2 milyon dollar vәsaiti öz hesabına vә ya digәr hesablara köçürüb. [1].

Nәhayәt, Melissa Virusu, Mafiaboy Hücumları, The Equifax Data Breach, The Sony Pictures Hack, The Target Data Breach, The Yahoo Data Breaches vә s. adlarla ifadә edilәn haker hücumlarının xarakterlәri dәyişәrәk e-maillәrin

virusla bulaşdırılması, Amazon kimi alış-veriş saytlarının çökdürülməsi, milyonlarla şəxsin fərdi məlumatlarının oğurlanması, kino senayesinə aid sirlərin ələ keçirilməsi, milyonlarla şəxsin debet kartlarının şifrələrinin çözülməsinin səviyyəsi [2] göstərdi ki, hücumlar artıq üç səviyyəyə qədəm qoyub:

- Fərdlərə
- Bizneslərə
- Hökumətlərə

Cəmiyyətin sosiologiyası adətən dövrün müasir texnologiylarının tətbiqi prosesinə hələ də izah edilməsi mümkün olmayan bir formada adaptasiya göstərir.

2007-ci ildən etibarən sosial şəbəkələrin meydana çıxması həm icmalardakı sinergetik vəziyyəti dəyişdirdi, həm yeni texologiyaları təsir və təzyiq aləti kimi istifadə edə bilən şəxslərin məqsədlərini dəyişdirdi, həm də informasiyaya mövcud olmuş ənənəvi baxışları dəyişdirdi.

Üç yeni kateqoriya dəyişikliyi dərhal təhlükəsizlik spektrində boşluqlar aşkar edə bildi. Xüsusilə də sosial media 2010-2012-ci illər arasında Yaxın Şərq və Şimali Afrikada baş verən bir sıra etiraz və üsyanlarda, "Ərəb Baharı"nda mühüm rol oynadı. "Facebook", "Twitter" və "YouTube" kimi sosial media platformaları "Ərəb Baharı" zamanı etirazçılar tərəfindən mesajlar təşkil etmək və çatdırmaq üçün istifadə edildi.

Bütün cəmiyyətlər üçün xarakterik olan iqtisadi, siyasi və sosial faktorlar ərəb dünyasında ilk dəfə sosial şəbəkələrin sayəsində təşkil edilmiş, məqsədyönlü aksiyalara çevrilərək, Tunisdə, Misirdə, Liviyada, Yəməndə hakimiyyət dəyişikliklərinə səbəb olmaqla yanaşı, Suriyada hələ də davam edən vətəndaş müharibəsinə şərait yaratdı.

Bu keys bizim üçün ən azı iki nəticə çıxartmağa imkan verir:

1. Sosial şəbəkələr – müasir anlayışla informasiya müharibəsinin aləti kimi ilk eksperimentdən uğurla keçdi.
2. "Ərəb Baharı"nda sosial medianın rolu akademik dairələrdə geniş müzakirə olunub, bəzi alimlər sosial medianın səfərbərlik, səlahiyyətləndirmə, fikirlərin formalaşdırılması və dəyişikliyə təsir göstərməsində kritik rol oynadığını, digərləri isə baş verən proseslərin sosial media şirkətlərinin siyasətinin olduğunu iddia edir.

Keys: Meta şirkətinin bu günlərdə Avropada 1,2 milyard avro cərimələnməsinə səbəb irlandiyalı istifadəçilərin məlumatını ABŞ-a ötürməsi olub. Nəzərə alsaq ki, İrlandiyanın 5 milyon əhalisi var və britaniyalı ingilislərlə bir yerdə yaşamaqdadırlar. Burada xeyli mübahisəli suallar meydana çıxır və ilk növbədə bizim də bəzi qayğılarımız yaranır. [3] [4].

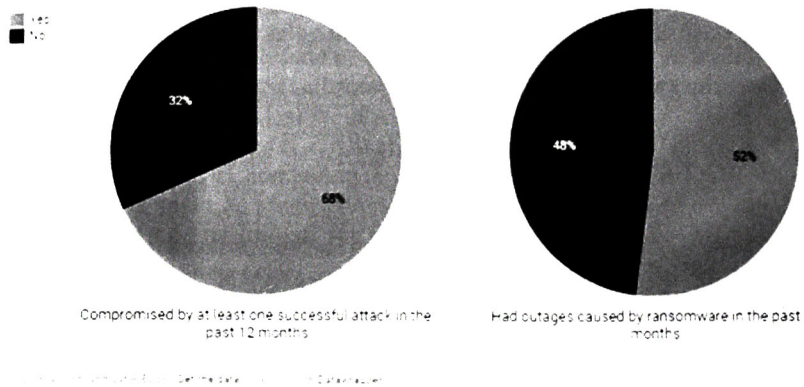
Lakin niyəsə günümüzdə əksər dövlətlər bu proseslərdə kvazi-haker rolunu icra etdiklərinə dair fikir bildirməyə tələsmirlər.

Amma 2022-ci ilin 24 fevral günü başlayan Rusiya -Ukrayna müharibəsi informasiya sərhədləri daxilində kiber müharibənin də başlaması ilə əlamətdar oldu.

Biz artıq hədəf rolunda gördüyümüz üst qurumun - dövlətin haker kimi fəaliyyət göstərdiyi dövrə qədəm qoymuş olduq.

"CyberEdge" kibertəhlükəsizlik araşdırmaları və marketinq konsaltinq şirkətinin hesabatına görə son bir ildə dünyanın əksər hökumətləri haker hücumuna məruz qalıb. [5]

Cybersecurity in the Public Sector



Şirkətin 17 ölkədə, 1200 dövlət və özəl sektor İT nümayəndələri arasında apardığı sorğu tədqiqatına görə, 2021-ci il ərzində sözügedən respondentlərin çalışdığı qurumların haker hücumlarına məruz qalma faizi 68,2 kimi yüksək təhlükəli rəqəm təşkil edir.

Maraqlıdır ki, kritik informasiyaların və dövlət sirrinin toplandığı mərkəzi server sistemlərindəki vəziyyət olduqca pis imiş. Belə ki, hökumət qurumlarının tez-tez hakerlərin hədəfinə çevrilməsinin ən əsas səbəbi onların zəif müdafiəsi, aşağı İT büdcəsi və məhdud İT heyətinin olmasıdır. [6]

Haker hücumları dövlətlərarası xarakterə keçən andan etibarən yeni terminlə ifadə edilir - kibermüharibə.

ABŞ və Çin arasında hazırda baş verən kiberhücumlar dövlətlərarası səviyyədə baş verən kibermüharibəyə ən aşkar nümunə sayıla bilər.

Problem o qədər ciddir ki, ilk dəfə sabiq ABŞ prezidenti Obama "Bu an üçün Amerikanın sülhü və rifahı kibertəhlükəsizlikdən asılı vəziyyətdədir" deyərək kibertəhlükəsizliklə bağlı yeni dövrə vurğu etdi.

Lider kiberhücum dövlətləri ilə yanaşı kiberdünyada Hindistan, Rusiya, Çexiya, Ukrayna, Almaniya, İndoneziya və Yaponiya kimi dövlətlərin bir-biri ilə rəqabət apardığını görürük.

Bir sözlə, kiberhücum mühiti dövlətləri bu sahədə milyonlarla dollarlıq büdcə ayırmağa məcbur edir. Kiberhücumlar dövlətlərarası olduğu zaman kibermüharibə baş verir. Kibermüharibədə kiberhücumlar hərbi məqsədlər və kibercasusluq, həmçinin məlumat sızdırmaq, təhlükəsizlik zəifliklərini tapmaq, qorxutma, siyasi və iqtisadi səbəblər kimi məqsədlərlə həyata keçirilə bilər. [7]

Kibermüharibələr bizim ənənəvi müharibə baxışlarımızı dəyişdirdi və onun yeganə fərqinin rəqəmsal dünyada baş verməsi ilə yanaşı, insan ölümü ilə nəticələnməməsi kimi də ifadə edilir.

Amma artıq bu yanaşma da geridə qaldı desək, səhv olmaz.

Belə ki, kibermüharibələrdə telefon dinləmələri, məxfi sənədlərə baxmaq və casusluq kimi xüsusi məqsədli əməliyyatların ön plana çıxdığını söyləyə bilərik. Amma süni və ağıllı intellektin son versiyalarının ortaya çıxması ilə artıq ölümlərin də baş verdiyini görə bilərik.

Məsələn, rus hakerlərinin Visat peyk sistemini bloklaması Polşada internet əlaqəsini kəsərək, qruplar arasındakı koordinasiyaya mane olmuş və hücum planının lokal uğursuzluqlarına səbəb olaraq itkilərlə nəticələnmişdir. [8]

Hazırda Ukrayna ilə Rusiya arasında DDOS, WhisperGate, HermeticWiper, IsaacWiper, UNC1151, APT28, Gameredon, Anonymos, İT Army of Ukraine, RU-Ransom Wiper və s. adlı haker qrupları müharibədə ön plana çıxmaqdadırlar. Hədəflər isə Müdafiə Nazirlikləri, müxtəlif güc strukturları, hərbi idarələr, maliyyə idarələri, məxfi sənədlər və s. -dir.

Daha bir ciddi məsələ süni intellektlə bağlıdır ki, bu məsələdə əsasən korporasiyaların adları və sahibləri ön plana çıxsalar da qərar tutduqları ölkələr, xüsusilə də ABŞ, Çin və ya Rusiyanın bu "uğurlardan" müəyyən məqsədlər üçün istifadə etdikləri müşahidə olunur.

Süni intellektin ərsəyə gətirdiyi "The Creator" (Yaradan) filmi ilk saatlarda 4 milyon izlənmə ilə rekord əldə etdi. [9]

Eyni tarixdə ABŞ-ın Montana ştatı ilk olaraq "TikTok" sosial şəbəkəsini qadağan etdi. [10]

Hətta iş o yerə çatıb ki, süni intellektin yaradıcısı, OpenAİ şirkətinin rəhbəri Sam Altman ABŞ konqrensində bu sahənin tənzimlənməsi ilə bağlı çıxışı zamanı qeyd edib ki, "əks təqdirdə qısa müddətdə onun girovuna çevriləcəyik". [11]

Şübhəsiz ki, Ermənistanın qanunsuz işğalı ilə başlayan müharibə Azərbaycan Respublikasının qələbəsi ilə başa çatsa da, kiberfəzada iki dövlət arasında mübarizə yeni-yeni alovlanmağa başlayıb.

Davamlı şəkildə "deepfake" (saxtakarlıqlar) ilə ölkəmizin hədəfə alınması amansız bir forma almaqdadır.

İlk növbədə dünya İT şirkətlərinin menecerləri sıralamasına baxanda görə bilərik ki, İran, Hindistan və Ermənistandan olan şəxslər Azərbaycana qarşı aparılan bu prosesdə rəhbər vəzifələrdə yer almaqdadırlar.

Hər üç ölkənin müəyyən yaxınlığını nəzərə alsaq, bizim üçün təhlükənin miqyası və xəritəsi dərhal böyüməkdədir.

Son olaraq 19 may tarixində Azərbaycanda 6500-dən artıq istifadəçi hakerlərin qurbanına çevrildi. [12]

"Azərbaycanda Kibercinayət və Kibertəhlükəsizlik Barometri" adlı kəmiyyət və keyfiyyət əsaslı (2021-2022-ci illərdə) təhlil aparan Sosial Tədqiqatlar Mərkəzinin analitik hesabatında yer alan "Kibercinayət barədə məlumatınız varmı" sualına 37. 1 faiz "bəli", 62,8 faiz isə "xeyr" kimi qorxunc bir cavab verib.

Və ya respondentlərin (ölkənin bütün iqtisadi rayonları üzrə təsadüfi seçilmiş 2283 nəfər və spesifik sahələr üzrə ekspertlər) 86,7 faizi ona qarşı nə vaxtsa kiber cinayət əməlinin olmasını hiss etməyib. 46,7 faiz isə "Fişinq" haqda heç bir məlumatının olmadığını ifadə edib.

"Ransomveə" (sistemə zərərli proqram köçürməsi) haqda isə əhalinin 97 faizinin məlumatı yoxdur. Sorğu göstərir ki, ölkədə 65 faiz İT üzrə işçinin təhlükəsizlik üzrə sığortası yoxdur və ya İT büdcəsindən kibertəhlükəsizliyə xərclənən maliyyə barədə 60 faizdən çox istifadəçi heç bir informasiyaya malik deyil.

Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin hesabatına görə Azərbaycanda kiberhücumların artım tempi ildə 38 faiz təşkil edir. [13]

Maraqlıdır ki, Vətən müharibəsində əldə edilən qələbədən sonra atılan addımlardan biri azad edilən rayonlarda "Ağıllı kənd"lərin salınması oldu. Yüsək texnoloji resurslarla ərsəyə gələn yeni tipli kəndlərin rəqəmsal mahiyyəti və ideoloji mənası onu dərhal qonşu dövlətin kiber hədəfinə gətirmiş oldu. Hazırda Azərbaycanda informasiya cəmiyyətinin inkişafına dair Konsepsiya, Gələcəyə baxış - yol xəritəsi, Dövlət sirri haqda qanun, Milli Təhlükəsizlik Konsepsiyası, kibercinayətkarlıq haqda qanun və onlarla müvafiq hüquqi aktın sırasında ən son qəbul edilən "Kritik informasiyanın qorunmasına dair" prezident fərmanı mühüm hüquqi-normativ baza formalaşdırıb.

Eyni zamanda Azərbaycanda İsrail institutu ilə birgə Kibertəhlükəsizlik Mərkəzi yaradılıb. Bu da yeni hərbi-siyasi, regional və qlobal nizam fonunda ölkəmiz üçün dördüncü fəzada – kibersferada mühüm nailiyyətlər vəd edir.

Nəticə:

Dövlət tərəfindən maliyyələşdirilən və həyata keçirilən kibermüharibə ənənəvi kiberterrorizmdən fərqlənməyə başlayır. Çünki o, kiberhücumları birbaşa planlaşdırıb həyata keçirən və ya digər ölkələrdəki muzdlulara himayədarlıq edən əcnəbi hökumət tərəfindən törədilir.

Başqa sözlə, dövlət tərəfindən dəstəklənən kibermüharibə bir hökumətin və ya dövlətin digər dövlətə, onun təşkilatlarına və ya şəxslərinə qarşı kiberhücumları dəstəklədiyi və ya həyata keçirdiyi kibermüharibə formasıdır.

Dövlət tərəfindən maliyyələşdirilən kiberhücumlar birbaşa olaraq hərbi və ya xüsusi dövlət orqanlarında işləyən hakerlər tərəfindən həyata keçirilir. Dövlət tərəfindən maliyyələşdirilən kiberhücumlar çox vaxt maliyyə qazancından artıq iqtisadi, siyasi və ya hərbi məqsədlərlə icra edilir. Dövlət tərəfindən maliyyələşdirilən kiberhücumların mənbəyini əksər hallarda tapmaq mümkün deyil, yəni kiberhücumun arxasında dövlətin olduğunu sübut etmək çətin ola bilər.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT

1. Famous Hacking Incidents and Their Implications (March 27, 2023) https://www.tekedia. com/famous-hacking-incidents-and-their-implications/
2. 27 Most Notorious Hacks in History that Fall Under OWASP Top 10 (March 28, 2023) https://www. indusface. com/blog/notorious-hacks-history/

3. Facebook owner Meta fined a record €1. 2 billion over European data transfers (Oct. 28, 2021.) https://www. euronews. com/next/2023/05/22/us-tech-giant-meta-fined-a-record-12-billion-in-europe
4. The social media myth about the Arab Spring (27 Jan 2021) https://www. aljazeera. com/opinions/2021/1/27/the-social-media-myth-about-the-arab-spring
5. Most Governments Were Hacked in the Past Year, Reports Reveal (April 18, 2022) https://www. govtech. com/security/most-governments-were-hacked-in-the-past-year-reports-reveal
6. Siber Saldırı Önlemede Blokzinciri Teknolojisinin Fayda Maliyet Açısından Değerlendirilmesi (2020) https://dergipark. org. tr/tr/download/article-file/1112079
7. Siber Saldırı Nedir? Siber Saldırılardan Nasıl Korunuruz? (3 Mart 2021) https://berqnet. com/blog/siber-saldiri
8. Polish Cyber Defenses and the Russia-Ukraine War (January 18, 2023) https://www. cfr. org/blog/polish-cyber-defenses-and-russia-ukraine-war
9. The Creator - https://www. youtube. com/watch?v=573GCxqkYEg&ab_channel=20thCenturyStudios
10. Governor Greg Gianforte - https://twitter. com/GovGianforte/status/1658948119285964802?t=-Xe79bvI13E4MwdqLDnRmQ&s=19
11. OpenAI CEO warns Senate: 'If this technology goes wrong, it can go quite wrong' (May 16, 2023) https://abcnews. go. com/Business/openai-ceo-warns-senate-technology-wrong-wrong/story?id=99357748
12. Bu dövlət qurumları haker hücumuna məruz qalıb – Siyahı https://qafqazinfo. az/news/detail/bu-dovlet-qurumlari-haker-hucumuna-meruz-qalib-siyahi-400874
13. «Azərbaycanda kibercinayət və kibertəhlükəsizlik barometri» açıqlandı https://www. youtube. com/watch?v=eXh9OlGY478&ab_channel=STMTV

Aziz Alibeyli,

The New State Model: From Hackerstate to New Security Concerns

Summary

The article touches on the new qualities of the cyber world, reveals the new details it covers. The emergence, development and current state of the cyber world are explained. The concept of state hacking in modern world is explained. At the same time, in the context of the emerging new world order, cyber attacks are viewed as an aspect of national security, as part of information warfare.

Quantitative and qualitative analysis, comparison method and historical sequence methods were used in the article.

Keywords: Cybercrime, cyberterrorism, cyberstate, social networks, information warfare

Азиз Алибейли

Новая государственная модель: от хакерского государства к новым проблемам безопасности

Резюме

Статья затрагивает новые качества кибермира, раскрывает новые детали, которые он освещает. Объясняется возникновение, развитие и современное состояние кибермира. Объясняется поня-тие государственного взлома в современном мире. При этом в условиях формирующегося нового мирового порядка кибератаки рассматриваются как аспект национальной безопасности, как часть информационной войны.

В статье использованы количественный и качественный анализ, метод сравнения и методы исторической последователь-ности.

Ключевые слова: Киберпреступность, кибертерроризм, ки-бергосударство, социальные сети, информационная война.