Dövlətin Kibersuverenliyinin Təmin Olunmasında Kibertəhdid Kəşfiyyatı və Əks-Kəşfiyyatı Texnologiyaları: Konseptual Yanaşmalar, Arxitektur Həllər və Perspektivlər

Adilə Kərimova
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
adila.karimova@aztu.edu.az

***Xülasə*— Rəqəmsal texnologiyaların, elektron hökümət xidmətlərinin, kritik informasiya infrastrukturunun sürətlə inkişafı kibertəhdidlərin miqyasını və mürəkkəbliyini ciddi şəkildə artırmışdır. Dövlət səviyyəsində kibertəhdid kəşfiyyatı texnologiyaları kibertəhdidlərin erkən aşkarlanması, analizi, risk idarəetməsi və proaktiv müdafiə mexanizmlərinin formalaşmasını təmin edir. Əks-kəşfiyyat texnologiyaları isə dövlətin təhlükəsizliyini təmin etmək üçün dövlətin informasiya resurslarını hədəf almış gizli fəaliyyətləri aşkarlayır, təhdid aktorlarını izləyir və kəşfiyyat fəaliyyətlərinə qarşı mübarizə aparır. Konseptual çərçivədə kibertəhdid kəşfiyyatı sistem arxitekturası strateji, operativ və taktiki səviyyədə strukturlaşdırılmış və inteqrasiya olunmuş model əsasında qurulmalıdır. Bu sistemin sintezi üçün süni intellekt metod və alqoritmlərinin işlənməsi dövlətin kibertəhlükəsizliyinin dayanıqlılığının təmin olunmasına və kibersuverenliyin gücləndirilməsinə xidmət edir.**

Açar sözlər— dövlətin kibersuverenliyi; kibertəhdid kəşfiyyatı; kibertəhdid əks-kəşfiyyatı; konseptual model.

I. GİRİŞ

Son illərdə dövlət və korporativ təşkilatlara qarşı yönəlmiş kiberhücumlar əhəmiyyətli dərəcədə artmış, geniş ictimai diqqətə səbəb olmuş və müvafiq elmi tədqiqatları aktuallaşdırmışdır. Bu hücumlar hal-hazırda daha mürəkkəb və təkmil metadologiyalarla həyata keçirilir. Kibercinayətkarların öz taktika, texnika və prosedurlarını yüksək səviyyədə təkmilləşdirmələri onların hüquq-mühafizə orqanları tərəfindən aşkarlanmasını və erkən mərhələdə qarşısının alınmasını çətinləşdirir.

Rəqəmsal transformasiya mühiti, kibermüharibənin sürətlə inkişafı və kibertəhdidlərin intensivləşməsi və əhəmiyyətli dərəcədə mürəkkəbləşməsi dövlətin milli maraqlarının qorunması üçün kibertəhdid kəşfiyyatı və əks-kəşfiyyatı texnologiyalarının formalaşmasını strateji zərurətə çevirir.

Kibertəhdidlərin daha mürəkkəb və təkmil metadologiyalarla həyata keçirilməsi, dövlətin kibersuverenliyinin təmin edilməsini, təhdid kəşfiyyatının gücləndirilməsini və rəqəmsal müharibəyə hazırlıq səviyyəsinin artırılmasını milli təhlükəsizlik prioriteti kimi qiymətləndirilir [1-3].

Mövcud kibertəhlükəsizlik konsepsiyaları dövlət səviyyəsində koordinasiya olunan kibertəhdidlərə qarşı effektiv mübarizə aparmaqda məhdudiyyətlərlə qarşılaşır. Bu kontekstdə intellektual və proaktiv müdafiə mexanizmlərinin formalaşdırılması müasir milli kibertəhlükəsizlik siyasətinin strateji istiqamətlərindən birinə çevrilir.

Kibertəhdid kəşfiyyatı (ing. Cyber Threat Intelligence – CTI) kritik infrastrukturların qorunmasında, milli təhlükəsizlik strategiyasının formalaşmasında və prioritetləşdirilməsində mühüm əhəmiyyət kəsb edir [2]. Dövlət səviyyəsində CTI komprometasiya indikatorlarının, təhdid aktorlarının taktika, texnika və prosedurlarının, davranış izlərinin sistemli analizini təmin edir. Beləliklə, CTI milli kibertəhlükəsizlik strategiyasının, kritik informasiya infrastrukturunun qorunmasının, risklərin proqnozlaşdırılmasının, dövlət siyasətinin konseptual və analitik arxitekturasının əsasını təşkil edir. Təhdid kəşfiyyatı proaktiv və reaktiv müdafiə mexanizmlərinin inteqrasiyasına imkan verir ki, bu da milli kibermüdafiə sisteminin dayanıqlılığına əhəmiyyətli dərəcədə təsir göstərir.

Dövlət səviyyəsində kibertəhdidlərin mürəkkəbliyi CTI ilə yanaşı əks-kəşfiyyat yanaşmalarının da vacibliyini aktuallaşdırır. CCI təhdid aktorlarının davranış modellərinin aşkarlanmasına, insidentlər arasında struktur və davranış uyğunluqlarını müəyyən etməyə, aktorların dezinformasiya və maskalanma mexanizmlərinin aşkarlanmasına, "saxta bayraq" (ing. false flag) əməliyyatlarının identifikasiyasına yönəlir. CTI və CCI bir-birini tamamlayan mexanizmlər hesab oluna bilər. CTI "təhdidi aşkarlamaq, analiz etmək, emal etmək, sistemləşdirmək və paylaşmaq" funksiyasını, CCI isə "təhdidi izləmək, manipulyasiya etmək, neytrallaşdırmaq" funksiyasını həyata keçirir. Bu iki mexanizmin inteqrasiyası texniki, idarəetmə və normativ uyğunluq baxımından düzgün təşkil olunmalıdır [4].

Bu məqalənin məqsədi dövlətin kibersuverenliyinin təmin olunması kontekstində dövlət–sektor–CERT modelinə əsaslanan CTI/CCI arxitekturasını konseptual şəkildə izah etməkdir. Nəticə etibarilə, CTI/CCI arxitekturası proaktiv

DOI: 10.25045/cyber.gov.2026.19

müdafiə mexanizmlərini və strateji qərarvermə prosesini gücləndirir. Bu yanaşma dövlətin kibersuverenliyinin daha strateji və adaptiv əsasda təmin etməyə imkan verir.

Kibertəhlükəsizlik artıq milli təhlükəsizlik strategiyasının tərkibinə daxil edilib, çünki kibərmüharibənin fiziki müharibə səviyyəsində ziyanlara səbəb ola biləcəyi sübuta yetirilibdir. Son zamanlar dövlət tərəfindən maliyyələşdirilən kiberkampaniyalar, fidyə proqramı hücumları və digər hücumlar kibertəhdidlərin yaratdığı dağdıcı təsiri açıq-aydın nümayiş etdirir. Bu hücumlar enerji, maliyyə sistemləri və kommunikasiya şəbəkələri daxil olmaqla mühüm sektorların mərkəzinə təsir edir. Belə fəaliyyətlərin dövlət sistemlərinə olan ictimai etimadın azalmasına, iqtisadi sabitliyin pozulmasına və bəzi hallarda hətta geosiyasi gərginliyin artmasına səbəb ola bilər. Nəticədə, kiberməkanda dövlətin kibersuverenliyinin təmin olunması ölkələr üçün aktual problemə çevrilib, bu da öz növbəsində kritik kibertəhlükəsizlik infrastrukturu və strateji yanaşmaların mövcudluğunu zəruri edir.

II. KONSEPTUAL ÇƏRÇİVƏ: KİBERTƏHDİD KƏŞFİYYATI (CTI) VƏ KİBER ƏKS-KƏŞFİYYAT (CCI)

Dövlətin kibersuverenliyinin təmin olunmasında təhdidləri aşkar etmək, onların mənbəyini, məqsədini və potensial təsirlərini analiz etmək lazımdır. Bu baxımdan CTI və CCI yanaşmaları strateji əhəmiyyət daşıyır və onların birgə tətbiqi proaktiv müdafiəni gücləndirir və qərarvermə prosesini daha effektiv edir. Kibertəhdidlərin artan miqyası onlardan qorunmaq üçün yeni təhlükəsizlik müdafiə strategiyası tələb edir. Təhdid kəşfiyyatı kibertəhdidləri qarşısını almaq və aradan qaldırmaq üçün kibertəhdidlər haqqında məlumatları aşkar edən, emal edən, analiz edən və paylaşan dinamik texnologiyadır. Təhdid kəşfiyyatı müdafiə arxitekturalarının müxtəlif səviyyələrini və qərar qəbuletmə mexanizmlərini dəstəkləyən aşağıda şərh edilən dörd əsas kateqoriyanı əhatə edir [1].

A. Strateji kəşfiyyat

Strateji kəşfiyyat operativ və taktiki kəşfiyyatdan fərqli olaraq, qlobal risk mühitinin, qurumlararası təhdid tendensiyalarının və geosiyasi dəyişikliklərin kibertəhlükəsizlik ekosisteminə təsirinin qiymətləndirilməsinə yönəlir. Bu kəşfiyyat dövlətin milli təhlükəsizlik əməliyyat mərkəzlərinin əsas hissəsi hesab olunur və dövlətin suverenliyinə, kritik infrastrukturuna və strateji oblektlərinə yönəlmiş kritik risklərin qiymətləndirilməsinə xidmət edir. Dövlət səviyyəsində strateji təhdid kəşfiyyatının əsas məqsədi təhdidlərin erkən aşkarlanması, milli maraqları hədəf almış risk senarilərinin modelləşdirilməsi və prioritetləşdirilməsi, siyasi qərar qəbuletmə mexanizminin təmin edilməsidir.

B. Taktiki kəşfiyyat

Taktiki kəşfiyyat əsasən operativ və detallı komprometasiya indikatorları (Indicators of Compromise – IoCs) formasında təqdim olunur və texniki səviyyədə proaktiv müdaxiləni dəstəkləyir. Taktiki kəşfiyyat məlumatlarına zərərli IP ünvanları, domen adları, URL-lər, fayl heşləri, imzalar və digər texniki artefaktlar daxildir. Bu məlumatlar dövlət qurumlarının təhlükəsizlik əməliyyat mərkəzləri və hüquq-mühafizə orqanları tərəfindən müdafiə mexanizmlərinin qurulmasında istifadə olunur. Bu səviyyənin əsas məqsədi təhlükəsizlik nəzarət mexanizmlərində real vaxt rejimində aşkarlama və zərərli davranışların erkən mərhələdə izolyasiyasını təmin etməkdir. Taktiki kəşfiyyat məlumatları müxtəlif mənbəli məlumat axınları vasitəsilə əldə edilir və avtomatlaşdırılmış təhlükəsizlik mexanizmlərinə inteqrasiya olunur. Bu səbəbdən, taktiki təhdid kəşfiyyatı müdaxilələri aşkarlama və cavab sistemləri üçün fundamental əhəmiyyət kəsb edir. Qeyd olunanlarla yanaşı, taktiki təhdid kəşfiyyatının əsas xüsusiyyətlərindən biri onun aktuallığını tez itirməsidir. Çünki zərərli domenlər və ya IP ünvanları vaxtaşırı dəyişdirilə və ya deaktiv edilə bilər.

C. Operativ kəşfiyyat

Operativ kəşfiyyat əsasən konkret təhdid aktoru, aktorun texniki imkanları və həmin aktorla əlaqəli təhdidlərin məcmusudur. Operativ təhdid kəşfiyyatı rəqib tərəfin davranışlarını, strateji məqsədlərini, istifadə etdiyi alətləri, resurs bazasını və kampaniya nümunələrini sistemli analiz edir. Bu kəşfiyyat, adətən, “kill-chain” modelinin analizini, zərərli proqram təminatının analizini, log analizləri, insident təhqiqat məlumatlarını özündə birləşdirir. Bu kəşfiyyatın əsas məqsədi təkcə ayrı-ayrı indikatorların aşkarlanması deyil, həmin indikatorları şərtləndirən davranış məntiqini kritik analiz etməkdir. Bu isə müdafiə mexanizmlərinin reaktiv və proaktiv şəkildə qurulmasına şərait yaradır.

D. Texniki kəşfiyyat

Texniki kəşfiyyat kritik informasiya infrastrukturlarının müdafiəsinə yönəlmiş təhdidlərin texnoloji istismar sistemlərini aşkarlamaq və onların qarşısını almaq üçün müdafiə mexanizmlərini formalaşdırmaqdır. Bu kəşfiyyat növü şəbəkə protocol anomaliyaları, “proof-of-concept” (PoC) nümunələri, proqram zəifliklərı və CVE-lər, tərs mühəndislik nəticələri, SCADA sistemləri, əməliyyat sistemləri, kriptoqrafik mexanizmlər kimi texniki biliklərin toplanmasına, analizinə və qiymətləndirilməsinə əsaslanır. Texniki təhdid kəşfiyyatı milli CERT strukturları, kibertəhlükəsizlik mərkəzləri, müdafiə orqanlarının xüsusi müdafiə qurumları tərəfindən həyata keçirilir.

Kiber əks-kəşfiyyat kəşfiyyat toplama (casusluq) və ya istismar cəhdlərinin qarşısını almaq üçün nəzərdə tutulmuş məqsədyönlü tədbirlər kompleksini əhatə edir. Başqa sözlə desək, CCI müdafiə sisteminə qarşı yönəlmiş kəşfiyyat və infiltrasiya cəhdlərinin neytrallaşdırılmasına istiqamətlənir. Dövlətin milli dayanıqlılığının təmin etdirilməsi üçün CCI-nin həm dövlət, həm də fərdi səviyyədə tətbiqi mühüm əhəmiyyət kəsb edir.

Kiber əks-kəşfiyyat “kəşfiyyat təşkilatı tərəfindən cinəyatkar təşkilatların kompüterlər, şəbəkələr və əlaqəli texniki avadanlıqlar vasitəsilə onlar haqqında həssas rəqəmsal məlumatların və ya kəşfiyyat məlumatlarını toplamasının qarşısını almaq məqsədilə həyata keçirilən tədbirlər” kimi müəyyən edilir. Başqa sözlə, CCI, məlumat toplamaq üçün kiber silahlardan istifadə edən kompüter əməliyyatlarını müəyyən edilməsi, onlara nüfuz edilməsi və ya neytrallaşdırması üçün həyata keçirilən tədbirlərdir. Bu

yanaşmada sızma faktının müəyyən edilməsinə, məhz bu sızmanın strateji məqsədinə və istifadə olunan metod və üsulların analizinə diqqət yetirilir. CCI müdaxilənin kontekstini və aktorun fəaliyyət modelini müəyyənləşdirməyi nəzərdə tutur [5].

Beləliklə, CTI əsasən təhdid haqqında bilik, CCI isə təhdid aktorunun davranışı prinsipinə əsaslanır. CCI və CTI-nin birgə tətbiqi dövlətin suverenliyinə aşağıdakı nəticələri formalaşdırır:

1) Strateji qərarvermə müstəqilliyi

2) Kritik infrastrukturun qorunması

3) Siyasi suverenlik

4) Proaktiv müdafiə

5) Risklərin düzgün qiymətləndirilməsi.

CCI və CCI-nin inteqrasiyası dövlətin kibersuverliyinin birgə tətbiqində strateji, institusional və siyasi təsir göstərir.

III. DÖVLƏT SƏVİYYƏSİNDƏ CTI/CCI ARXİTEKTURASI

Kibertəhdid kəşfiyyatı və kibər əks-kəşfiyyat yanaşmalarının inteqrasiyası dövlətin kibersuverenliyinin təmin olunması üçün zəruri faktordur. Bu kontekstdə təklif olunan arxitektura dövlət–sektor–CERT modelinə əsaslanır. Bu modelə görə təhdid məlumatlarının toplanması, emalı, strukturlaşdırılması, analizi və sektorlar üzrə paylanması vahid sistem kimi nəzərdə tutulur. Təklif olunan arxitekturanın əsas məqsədi milli kibertəhlükəsizlik ekosistemində müxtəlif təhdid aktorları təhdid məlumatlarını vahid qaydalarla paylaşır. Qeyd etmək lazımdır ki, nəzərdə tutulan paylaşım həssaslıq səviyyəsinə uyğun olaraq mərhələli şəkildə həyata keçirilir.

Milli CERT/Gov-CSIRT qurumu CTI-CCI arxitekturasının mərkəzidir və CTI və CCI analitik modullarının idarə olunması burada həyata keçirilir. Başqa sözlə, CTI prosesləri, insidentlərin korrelyasiyası, aktor davranışları mərkəzi sektorda həyata keçirilir (Şəkil 1). Mərkəzləşdirilmiş koordinasiya mexanizmi dövlət səviyyəsində milli kibertəhdid monitorinqini artırır və təhdidlərin sektorlar arasında yayılma riskini azaldır.

Arxitektura aşağıdakı əsas funksional qatlardan ibarətdir:

- Operativ qat
- Milli koordinasiya qatı
- Analitika qatı
- Məlumat idarəetmə qatı
- Çıxış və paylaşım qatı

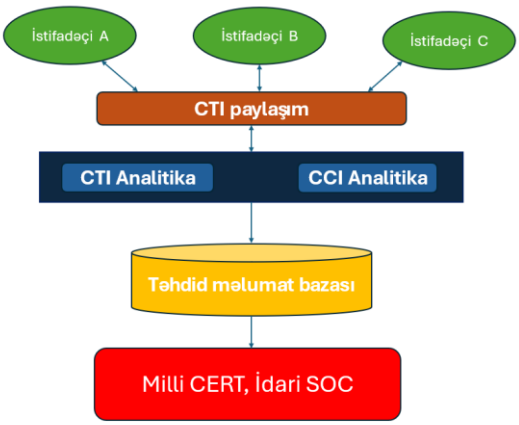
Operativ qat, yəni sektor qatı “xam məlumatın” əldə olunma qatıdır. Bu qatın tərkibinə İdari-SOC-lar, sektor CERT-ləri, dövlət qurumlarının təhlükəsizlik sektorları, kritik infrastruktur qurumları, enerji, bank, telekom sektorları, OSINT daxildir. Qeyd olunan sektorlardan daxil olan məlumatlara IoC-lar, insident hesabatları, log və telemetriya nümunələri, zərərli proqram artefaktları daxil ola bilər. İlkin mərhələdə məlumatlar normallaşdırılmalı və klassifikasiya olunmalıdır.

Milli koordinasiya qatı idarəedici və əlaqələndirici qat hesab olunur. Milli CERT / Gov-CSIRT daxil olan məlumatları zənginləşdirmə və korrelyasiya mərhələlərindən keçirir. Zənginləşdirmə mərhələsində xam IoC-lər əlaqəli heş və domenlər, ASN provayder, WHOIS məlumatı, sandbox analiz nəticələri, reputasiya məlumatları, MITRE ATT&CK uyğunluğu, insident məlumatları və davamlılıq mexanizmi ilə zənginləşdirilir. Korrelyasiya mərhələsində müxtəlif sektorlardan daxil olan məlumatlar birləşərək daha böyük sistemli hücum modeli formalaşır.

Analitik qat milli səviyyədə qərarvermə mexanizmlərini və CCI proseslərini əhatə edir. Bu qat məlumatı kəşfiyyata çevirir. Analitika qatı CTI Analitika və CCI Analitika olmaqla iki hissədən ibarətdir. CTI analitikada taktiki və operativ analizi, IoC-ların sistemli analizi, TTP uyğunlaşdırmaları həyata keçirilir. CCI qatında isə “false flag” risklərinin qiymətləndirilməsi təhdid aktorunun fəaliyyət infrastrukturunun izlənməsi, actor identifikasiyası aparılır. Analitik qatda texniki bilik, strateji analiz və operativ koordinasiya tələb olunur. Bu səbəbdən CCI qatı Milli CERT və milli təhlükəsizlik səviyyəsində fəaliyyət göstərən mexanizmlərlə inteqrasiya olunmalıdır.

Məlumat İdarəetmə qatı bilik mərkəzi hesab olunur və bu məlumat bazasında İOC-lar saxlanılır, kampaniyalar arxivləşdirilir, aktor profilləri toplanılır.

Çıxış və paylaşım qatı arxitekturanın effektivliyini təmin edən qat hesab olunur və 3 hissədən ibarətdir: Taktiki CTI, Strateji CCI, CTI Paylaşım & TLP. Təklif olunan modeldə məlumatlar TLP (Traffic Light Protocol) səviyyələri və “need-to-know” prinsipi əsasında paylaşılır. Məsələn, TLP:RED səviyyəli məlumatlar yalnız məhdud auditoriya üçün nəzərdə tutulur və sektorlararası geniş paylaşım edilmir; TLP:AMBER səviyyəsində isə sektor daxilində koordinasiyalı xəbərdarlıqlar mümkündür; TLP:GREEN və TLP:CLEAR səviyyələri daha geniş paylaşımı dəstəkləyir. Bu mexanizm məxfilik və paylaşım səviyyəsinin idarə olunmasını təmin edir.



Şəkil 1. CTI/CCI arxitektursası

CTI/CCI arxitekturası kibersuverenliyin təmin olunması üçün aşağıdakı üstünlükləri yaradır:

- vahid milli kiberməkanın formalaşması;
- reaktiv müdafiədən proaktiv müdafiəyə keçid;
- sektorlararası yoluxmanın qarşısının alınması;
- strateji qərarvermə mexanizmi;
- etimad və koordinasiya ekosistemi.

NƏTİCƏ

Nəticə olaraq, təklif olunan CTI/CCI arxitekturasın dövlətin kibersuverenliyinin təmin edilməsi baxımından strateji yanaşma kimi qiymətləndirilə bilər. Gələcək tədqiqat və tətbiq istiqamətləri kimi süni intellekt əsaslı analitika, federativ CTI paylaşımı, threat hunting inteqrasiyasının tətbiqi perspektivli hesab olunur.

MİNNƏTDARLIQ

Bu iş Azərbaycan Texniki Universitetinin elmi-tədqiqat işlərinin və innovasiyaların dəstəklənməsi və inkişafı məqsədilə təqdim etdiyi daxili qrantın dəstəyi ilə həyata keçirilmişdir – Müqavilə № AzTU-DQL-2025-M01/60182631.

ƏDƏBİYYAT

[1] A. Kərimova, "Kibertəhdid kəşfiyyatının bəzi məsələləri haqqında," in *"Azərbaycanın təhlükəsizlik orqanları: tarixi inkişaf və müasirlik" mövzusunda respublika elmi-praktiki konfransının tezisləri*, Təhlükəsizlik orqanlarının yaradılmasının 105 illik yubileyinə həsr olunmuş, 2024, pp. 239–240.

[2] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, 2023.

[3] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," *Computers & Security*, vol. 87, p. 101589, 2019.

[4] M. U. Rana, O. Ellahi, M. Alam, J. L. Webber, A. Mehbodniya, and S. Khan, "Offensive security: Cyber threat intelligence enrichment with counterintelligence and counterattack," *IEEE Access*, vol. 10, pp. 108760–108774, 2022.

[5] M. Motlhabi, P. Pantsi, B. Mangoale, R. Netshiya, and S. Chishiri, "Context-aware cyber threat intelligence exchange platform," in *Proc. Int. Conf. Cyber Warfare and Security*, vol. 17, no. 1, 2022, pp. 201–210.

Cyber Threat Intelligence and Counterintelligence Technologies in Ensuring the State's Cyber Sovereignty: Conceptual Approaches, Architectural Solutions and Perspectives

Adila Karimova

Azerbaijan Technical University, Baku, Azerbaijan

Abstract— The rapid development of digital technologies, e-government services, and critical information infrastructure has significantly increased the scale and complexity of cyber threats. At the state level, cyber threat intelligence technologies provide early detection, analysis, risk management, and the formation of proactive defense mechanisms. Counterintelligence technologies, on the other hand, detect covert activities targeting state information resources, track threat actors, and combat intelligence activities to ensure state security. In the conceptual framework, the cyber threat intelligence system architecture should be built on the basis of a structured and integrated model at the strategic, operational, and tactical levels. The development of artificial intelligence methods and algorithms for the synthesis of this system serves to ensure the sustainability of the state's cybersecurity and strengthen cyber sovereignty.

Keywords— state cyber sovereignty; cyber threat intelligence; cyber threat counterintelligence; conceptual model.