Kiberdayanıqlılıq Konsepsiyası və Onun Kibersuverenliyin Təmin Olunmasındakı Rolu

Rauf İsmayılzadə
Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası, Bakı, Azərbaycan
ismayilzadehrauf2005@gmail.com

***Xülasə*— Kibertəhlükəsizlik informasiya və əməliyyat texnologiyalarının təhlükəsizliyi ilə sıx bağlı, müxtəlif texnika və anlayışları əhatə edən sahədir. Onun əsas xüsusiyyəti rəqibə qarşı hücum xarakterli İT strategiyalarının mümkünlüyüdür. Lakin terminın geniş və qeyri-dəqiq istifadəsi onu informasiya və ya İT təhlükəsizliyi ilə eyniləşdirərək yanlış anlaşılmalar yaradır və mühüm fərqləri kölgədə qoyur. Məqalə təklif edir ki, "kibertəhlükəsizlik" yalnız İT mühitində müdafiəyə yönəlmiş təcrübələri ifadə etsin. Tədqiqat kibertəhlükəsizlik, kibermüdafiə və kiberdavamlılıq əlaqəsini, yeni konseptual çərçivəni, həmçinin CRRT-in rolunu təhlil edir.**

Açar sözlər*— *kiber davamlılıq; kiber təhlükəsizlik; kibermüdafiə; kiber cavab qrupları.

I. GİRİŞ

Bununla belə, kibertəhlükəsizlik termini mənşəcə hərbi dairələrdən qaynaqlansa da, son on il ərzində əhəmiyyətli dəyişikliklərə məruz qalmışdır. Bununla yanaşı, bu anlayışın son dövrlərdə müxtəlif sahələrə yayılması onun mahiyyətinin qismən təhrif olunmasına səbəb olmuşdur. Kibertəhlükəsizlik təkcə informasiyanın mühafizəsinin təmin edilməsi ilə məhdudlaşmır. Buraya rəqəmsal aktivlərin qorunması məqsədilə əməliyyat texnologiyalarının (OT) təhlükəsizliyi və informasiya texnologiyalarının (İT) təhlükəsizliyi də daxildir. Kiber təhdidlərə qarşı effektiv müdafiə həssas hücum kanallarının cəlbediciliyinin azaldılması üçün kompleks tədbirlərin görülməsini, mühüm obyektlərin və məxfi məlumatların müəyyən edilməsini, hücumların daha baha başa gəlməsini təmin edən mühafizə mexanizmlərinin tətbiqini, hücumların etibarlı şəkildə aşkarlanması vasitələrinin hazırlanmasını və operativ əks-tədbirlərin planlaşdırılmasını tələb edir.

Bundan əlavə, bu, hücum yollarının və zəif nöqtələrin müəyyən edilməsi məqsədilə texniki sınaqlardan istifadə olunan kibermüdafiənin digər bir sahəsini də əhatə edir. Avropa İttifaqında kibertəhlükəsizlik dinamik təhdidlərə qarşı adaptiv tədbirlərin formalaşdırılması üçün məlumatlılıq, davamlılıq və cavabvermə prinsiplərinə əsaslanır. Eyni zamanda, zərərli fəaliyyətlərin aşkarlanması və daha dərindən anlaşılması imkanlarını artırmaq, habelə kritik infrastrukturun, cəmiyyətin və institutların davamlılığını gücləndirmək məqsədilə Aİ bu istiqamətdə səylərini intensivləşdirməyə çalışır. Bu yanaşma Avropa İttifaqının kiberhücumlara qarşı dayanıqlılığının möhkəmləndirilməsi və hücumlardan sonrakı bərpa prosesinin təmin edilməsi baxımından mühüm əhəmiyyət kəsb edir. Məhz buna görə də üzv dövlətlərin birgə fəaliyyət göstərməsi, eləcə də Avropa İttifaqı, onun üzv dövlətləri, tərəfdaş ölkələr və NATO arasında əməkdaşlıq mexanizmlərinin formalaşdırılması zəruridir.

Bu məqalənin məqsədi dəyişən təhlükəsizlik təhdidləri və məhdud əks-tədbirlər fonunda kibertəhlükəsizlik, kibermüdafiə və kiberdavamlılıq arasındakı qarşılıqlı əlaqə və dinamikaları araşdırmaqdır. Eyni zamanda, tədqiqat Avropa İttifaqının Kiber Sürətli Cavab Qrupları (Cyber Rapid Response Teams – CRRT) və Kibertəhlükəsizlik sahəsində Qarşılıqlı Yardım (Mutual Assistance in Cyber Security) mexanizmləri üçün nəzərdə tutulmuş normativ-hüquqi çərçivəni təhlil edərək, Aİ səviyyəsində kibertəhlükəsizlik və kibermüdafiəyə yeni bir baxış bucağı təqdim edir.

Məqsədlər

- Strateji baxışa və adaptiv təhlükələrə hazırlığa əsaslanaraq, ənənəvi kibertəhlükəsizlik yanaşmasından genişmiqyaslı kiberdavamlılıq konsepsiyasına keçidə diqqət yetirmək.
- Aİ çərçivəsində kiber hadisələrin idarə olunmasını gücləndirməyə və əməkdaşlığı təşviq etməyə yönəlmiş CRRT və Kibertəhlükəsizlik sahəsində Qarşılıqlı Yardım (MA in CyS) layihələrinin təkamülünün və funksionallığının icmalı.

II. METODOLOGİYA

Bu tədqiqat mövcud informasiya-kommunikasiya ekosistemində kibertəhlükəsizlik və kibermüdafiənin mürəkkəb mühitini, eləcə də kiberdavamlılığın formalaşdırılmasındakı rolunu hərtərəfli şəkildə araşdırmaq məqsədilə sistemli və modelyönümlü yanaşmanı tətbiq edir.

İlk mərhələdə bu tədqiqat araşdırılan mühitin ətraflı təhlilini əhatə edir. Daha sonra həmin mühitə qarşı mövcud ola biləcək risklərin müəyyən edilməsi məqsədilə kibermüdafiə təhlili aparılır. Bu təhlil potensial hücumların qarşısının alınmasına yönəlmiş müvafiq təhlükəsizlik strategiyalarının layihələndirilməsi və tətbiqi üçün əsas yaradır. Bu kontekstdə məqalə müasir informasiya-kommunikasiya mühitində kiberdavamlılıq anlayışına fərqli və alternativ bir baxış təqdim etməyi qarşıya məqsəd qoyur.

Bu tədqiqatın məqsədi müasir informasiya-kommunikasiya mühitində kiberdavamlılığın əldə olunmasına yönəlmiş şəkildə kibertəhlükəsizlik və kibermüdafiəyə dair müxtəlif baxış bucaqlarını təqdim etməkdir. Nəticə etibarilə, bu yanaşma unikal bir konseptual kiberdavamlılıq modelinin

DOI: 10.25045/cyber.gov.2026.38

formalaşdırılmasına gətirib çıxarır. Təqdim olunan model Avropa İttifaqının Kiber Sürətli Cavab Qruplarını (CRRT) kibertəhlükəsizlik problemlərinin mümkün həll yollarından biri kimi nəzərə alan innovativ kibertəhlükəsizlik modelinə dair yanaşma və elmi baxışları özündə ehtiva edir. Bu CRRT-lər insan resurslarının, əməliyyat imkanlarının və texnologiyaların paylaşılması yolu ilə qarşılıqlı yardım mexanizmi kimi fəaliyyət göstərir.

Kibermüdafiə çərçivəsində bu tədqiqat kiberhücumların və ya təhdidlərin qarşısının alınması, vaxtında aşkarlanması və operativ cavablandırılması kimi mühüm funksiyalara xüsusi diqqət yetirir. Əsas məqsəd infrastrukturun bütövlüyünün qorunmasını və həssas məlumatların müdafiəsini təmin etməkdir. Kiber təhdidlərin həcminin və mürəkkəbliyinin artması fonunda kibermüdafiə təşkilatlar və qurumlar üçün mühüm bir komponent kimi ön plana çıxır və proseslərin, eləcə də fəaliyyətlərin təhlükəsiz şəkildə, potensial təhdidlərin kölgəsi olmadan icrasına imkan yaradan mühit formalaşdırır. Bundan əlavə, kibermüdafiə xüsusilə kritik sahələrdə təhlükəsizlik resurslarının və maliyyə xərclərinin daha səmərəli istifadəsini təmin edir.

Kiber təhdidlər getdikcə daha da ağırlaşır və onların qarşısının alınması daha mürəkkəb xarakter alır. Məhz bu səbəbdən Litva Avropa İttifaqının Müdafiə Şurasına “Kiber Sürətli Cavab Qrupları və Kibertəhlükəsizlik sahəsində Qarşılıqlı Yardım” adlı layihə təklif etmişdir. Bu təşəbbüsün məqsədi həm Avropada, həm də ABŞ-da kibertəhlükəsizliyin səviyyəsini artırmaqdır. Layihənin əsas məqsədi iştirakçı ölkələrdən olan kibermüdafiə üzrə mütəxəssislərdən ibarət çoxmillətli sürətli cavab kiber qruplarının yaradılmasıdır.

Bu layihənin fərqləndirici cəhəti iştirakçı dövlətlər arasında resursların paylaşılmasına verdiyi xüsusi əhəmiyyətlə səciyyələnməsidir; bu isə əsasən informasiya mübadiləsinə fokuslanan mövcud çoxmillətli kibermüdafiə təşəbbüslərinin bir çoxunu geridə qoyur. Layihə çərçivəsində Avropa İttifaqında kibertəhlükəsizliklə bağlı hüquqi prosedurların tədqiqi, masaüstü təlimlərin (kiber böhran simulyasiyalarının) təşkili və kibermüdafiə alətlərinin hazırlanması nəzərdə tutulur. Mövcud vəziyyətə görə, altı Aİ üzv dövləti layihəyə qoşulmuşdur (Xorvatiya, Litva, Estoniya, Polşa, Niderland, Rumıniya), yeddi dövlət isə onun inkişafını müşahidəçi qismində izləyir (Finlandiya, Belçika, İtaliya, Fransa, İspaniya, Yunanıstan, Sloveniya) .

III. PROBLEMİN HƏLLİ

Getdikcə daha çox qarşılıqlı əlaqəli hala gələn rəqəmsal dünyada ənənəvi kibertəhlükəsizlik tədbirləri təkbaşına dəyişən kiber təhdidlər mənzərəsinə qarşı yetərli hesab edilmir. Müasir yanaşma müdafiə, qarşısının alınması və cavabvermə elementlərini özündə birləşdirən kompleks strategiyanı tələb edir; bu strategiya sadəcə təhlükəsizlik anlayışı ilə kifayətlənməyərək davamlılıq konsepsiyasını da əhatə etməlidir. Kiberdavamlılıq fundamental yanaşma kimi rəqəmsal şəbəkələşmiş sistemlərin yalnız hadisə zamanı deyil, həm də hadisədən əvvəl və sonra təhdidlərə qarşı davam gətirmə hazırlığını və imkanlarını qiymətləndirir. Qeyd etmək vacibdir ki, davamlılıq bərpa anlayışı ilə eyni mənanı daşımır;

Kiberdavamlılıq onun uzun müddət fəaliyyət göstərmə qabiliyyətinə əsaslanır. Güclü strategiya, potensial risklərin yaranma ehtimalını əvvəlcədən nəzərə alan və riskin baş verməsindən əvvəl, baş verərkən və sonra onu minimuma endirmək yollarını planlaşdıran uzunmüddətli yanaşmanı əhatə edir. Strategiyaların uzunmüddətli perspektivdən nəzərdən keçirilməsi onların tam və çevik olmasını təmin edir, beləliklə müxtəlif situasiyalarda effektiv işləyə bilir. Təhdidin bütün mərhələlərini nəzərə alan strategiyalar, yalnız müəyyən bir anı nəzərə alan yanaşmalara nisbətən təbii olaraq daha davamlı olur.

Rəhbərlik kiberdavamlılığın istiqamətini və inkişafını ən çox təsir edən faktordur. Adətən informasiya təhlükəsizliyi ilə bağlı aparılan müzakirələrin kənarına çıxmaq və bütün şəbəkələrin davamlılığı barədə daha geniş bir dialoq qurmaq vacibdir. Daha geniş baxış bucağı iqtisadiyyatın və cəmiyyətin problemləri idarə edə bilməsini təmin etmək üçün əhəmiyyətlidir. Bu, xüsusilə süni intellekt (AI), əşyaların interneti (IoT) və kvant hesablama kimi yeni texnologiyaların ortaya çıxması və yeni risklər yaratması fonunda aktuallığını qoruyur. Şirkətlər üçün sürətlə dəyişən texnologiyaların yaratdığı problemlərə qarşı uzunmüddətli planlamada çevik yanaşmanı daxil etmək xüsusilə vacibdir.

Kibertəhlükəsizliyin giriş nəzarəti komponenti ilə kiberdavamlılığın strateji və gələcəyə yönəlmiş düşüncə tərzi arasında nəzərəçarpan fərq mövcuddur. Kiberdavamlılıq anlayışı genişmiqyaslı yanaşmanı tələb edir və fokusun tək müəssisələrdən qarşılıqlı əlaqəli sistemlərə keçirilməsini nəzərdə tutur. Şəbəkələşmiş mühitdə bir düyündəki zəifliyin bütöv şəbəkənin təhlükəsizliyini və davamlılığını risk altına qoyma potensialı olduğunu başa düşmək vacibdir. Buna görə də, davamlılığın ictimai malların (public goods) və ya ümumi resursların çərçivəsində əhəmiyyətini, xüsusilə əməkdaşlıq dəyərini nəzərə almaq zəruridir. Bu münasibətlər yalnız kommersiya müəssisələrini deyil, həm də tənzimləyici orqanları, hüquq-mühafizə qurumlarını və dövlət rəsmilərini əhatə edə bilər və beləliklə kiberdavamlılığın yaradılması və saxlanılması üçün ortaq ehtiyacı nümayiş etdirir.

Kiberdavamlılıq anlayışı təbii olaraq risklərin idarə olunması prinsiplərinə əsaslanır və aydın müəyyən edilmiş başlanğıc və ya son mərhələyə malik deyil. Lakin strateji metodologiyanın inkişafı və risk transfer mexanizmlərinin həyata keçirilməsi nəticəsində bu anlayış transformasiyaya uğrayır. Həm özəl sektor, həm də dövlət qurumlarının rəhbərləri kiber təhdidlərin qarşısının alınması və minimuma endirilməsinin vacibliyini dərk etmək məsuliyyətini daşıyırlar. Kiberdavamlılığın artırılması üçün maraqlı tərəflər arasında əməkdaşlığın inteqrasiyası əsasdır. Lakin bu əməkdaşlığın effektiv şəkildə planlaşdırmaya daxil edilməsini təmin etmək təşkilati rəhbərlərin məsuliyyətidir.

Tarixi baxımdan, kibertəhlükəsizlik strategiyaları əsasən mövcud və tanınmış təhdidlərin qarşısının alınmasına yönəlmişdir ki, bu da hərtərəfli kibertəhlükəsizlik çərçivəsinin ayrılmaz elementi olaraq qalır. Bununla belə, sürətlə dəyişən kiber təhlükələr mühitində, eyni dərəcədə vacib olan, naməlum riskləri qabaqcadan proqnozlaşdırmaq, onları müəyyən etmək və öyrənmək üçün inkişaf etmiş bacarıqların formalaşdırılmasıdır. Hər bir təhlükəsizlik problemi, onun tanış

və ya yeni olmasından asılı olmayaraq, fərdi həll yoluna malikdir. Sistem təhlükəsizliyinin sistemli qiymətləndirmələrindən əldə olunan dəyərlərin inteqrasiyası vasitəsilə bu məsələlər "məlum məlumlar" (informasiya təhlükəsizliyi ilə bağlı), "məlum məlumlar" (kibertəhlükəsizlik ilə bağlı) və "naməlum naməlumlar" (kiberdavamlılıq ilə bağlı) kimi təsnif edilə bilər.

Konseptual Kiberdavamlılıq Modelinin təqdim olunması kiberdavamlılığı anlamaq və praktikada tətbiq etmək üçün strukturlaşdırılmış yanaşma yaratmaq məqsədini daşıyır. Bu tədqiqatın təqdim etdiyi model üç müstəvidən ibarətdir: informasiya təhlükəsizliyi, kibertəhlükəsizlik və kiberdavamlılıq.

Informasiya təhlükəsizliyi müstəvisi üç əsas komponentdən ibarətdir: əlyetərlilik (availability), tamlıq (integrity) və məxfilik (confidentiality). Bu üç komponent tez-tez "CIA triadı" adlandırılır və bu hissədə CIA triadı ilə bağlı təhdidlər və onlara cavab tədbirləri öyrənilir.

Kibertəhlükəsizlik müstəvisi isə CIA triadına uyğun gəlməyən daha mürəkkəb təhdidlərə yönəlib. Buraya Qabaqcıl Davamlı Təhdidlər (Advanced Persistent Threats – APTs) və onlara qarşı qorunma yolları daxildir.

Nəhayət, kiberdavamlılıq müstəvisi proqnozlaşdırmaq və idarə etmək mümkün olmayan təhdidləri, habelə onlarla mübarizə üsullarını əhatə edir.

Sistemlər tez-tez qarşıya çıxan gözlənilməz problemlərlə mübarizə aparmaq üçün insanların iş proseslərini dəyişdirmək, yeni təşkilati üsullar yaratmaq və yeni texnologiyalar tətbiq etmək bacarıqlarını dəstəkləyir. Kiber risklər artdıqca sistemlər dəyişməli və əməkdaşlara mövcud prosesləri, təşkilatları və texnologiyaları dəyişdirmək imkanı verilməlidir. Sistemlər gözlənilməz hadisələrə çevik şəkildə uyğunlaşa və reaksiya verə bilməlidir. Kiberdavamlılığın mühüm komponentlərindən biri planlaşdırılmamış hadisələrə adaptasiya bacarığıdır. Bu, müəssisələrin yeni situasiyaları uğurla idarə etməsini və əməliyyat bütövlüyünü qorumasını təmin edir.

Avropa İttifaqının Kiber Sürətli Cavab Qruplarının (CRRT) və Kibertəhlükəsizlikdə Qarşılıqlı Yardım layihəsinin birgə işləməsi güclü kiber infrastrukturun yaradılmasına yönəlmiş çox innovativ addımdır. Bu, Aİ-nin Daimi Strukturlaşmış Əməkdaşlıq (PESCO) çərçivəsində təsdiqlənmiş ən qabaqcıl layihələrdən biridir. PESCO-nun məqsədi xüsusi hərbi öhdəlik və imkanlara malik Aİ üzv dövlətləri arasında təhlükəsizlik və müdafiə əməkdaşlığını gücləndirməkdir.

"Kiber Sürətli Cavab Qrupları və Kibertəhlükəsizlikdə Qarşılıqlı Yardım" sahəsində niyyət bəyannaməsi insanların kibermühitdə könüllü şəkildə əməkdaşlığının vacibliyini vurğulayır. Məlumat mübadiləsi, birgə təlimlər, əməliyyatlarda qarşılıqlı yardım, elmi-tədqiqat fəaliyyəti və birgə imkanların qurulması bu əməkdaşlığın əsas elementləridir. Mütəxəssislər, onların müntəzəm Kompüter Təhlükəsizliyi və Cavab Qrupları (CSIRTs) və CRRT-ləri vasitəsilə, CSIRT Şəbəkəsi, Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi (ENISA) və CERT-EU kimi Aİ təşkilatları ilə birgə işləyərək mövcud kibertəhlükəsizlik təşəbbüslərini dəstəkləyirlər.

CRRT-lər üzv dövlətlərin razılaşdığı çərçivə daxilində fəaliyyət göstərir, mülki-hərbi təbiətə malikdir, kiberdomendə əməkdaşlıq mədəniyyətini təşviq edir və Aİ daxilində kibermüdafiə anlayışını genişləndirir. Avadanlıqların təkmilləşdirilməsi də nəzərdə tutulur; məqsəd kibertəhdidləri aşkar edən, tanıyan və azaltmaq üçün ümumi Kiber Alətlər Dəstinin (Cyber Toolkit) yaradılmasıdır. Bu alətlər dəstəyinin hazırlanması üçün Avropa Müdafiə Fondu və digər Aİ maliyyə mənbələri araşdırılır, iştirakçı üzv dövlətlər arasında sənaye əməkdaşlığı təşviq edilir və Avropa kibertəhlükəsizlik sənayesi gücləndirilir.

2020-ci ilin yanvarında Anlayış Memorandumunun uğurla imzalanması mühüm mərhələni qeyd etdi və CRRT-lər 2021-ci ildə tam əməliyyat qabiliyyətinə çatdı. Layihə üzrə lider ölkə kimi Litva Respublikası Milli Müdafiə Nazirliyi fəaliyyət göstərir, bu isə daha geniş miqyasda kiberdavamlılığın gücləndirilməsi üçün tələb olunan əməkdaşlıq ruhunu nümayiş etdirir.

IV. MÜZAKİRƏ

Müasir cəmiyyətlər kommunikasiya və informasiya texnologiyaları ilə ayrılmaz şəkildə əlaqələnmişdir; insanlar müxtəlif texnologiyalar vasitəsilə mətni, şəkilləri və səsi paylaşaraq bir-biri ilə qarşılıqlı əlaqədədir. Bu qarşılıqlı əlaqə, o cümlədən Əşyaların İnterneti (IoT) texnologiyalarının genişlənən təsiri, bu sistemlərin düzgün işləməsindəki sapmaları sadəcə texniki nasazlıqlar olmaqdan çıxarıb qlobal təhlükəsizlik təhdidlərinə çevirmişdir. Nəticədə, cəmiyyətlər bu təhdidlərə qarşı çıxmaq üçün "kibertəhlükəsizlik" adı altında kollektiv şəkildə həyata keçirilən hərtərəfli tədbirlər və fəaliyyətlər sistemini formalaşdırmışdır.

Kiber risklərə effektiv cavab verməyin əsas açarı onların normallaşdırılmasındadır. Kiber risklər, təşkilatların məqsədlərinə nail olmaq üçün idarə etməli olduğu digər risklər kimi qəbul edilməlidir. Biznes və dövlət rəhbərləri davamlılığa (resilience) yönəlmiş düşüncə tərzini iki mühüm səbəbə görə mənimsəməlidir. Birincisi, bu yanaşma yalnız şəbəkə pozuntularının qarşısını almağa fokuslanan "hamısı və ya heç nə" prinsipi ilə bağlı fəlakətli nəticələrin qarşısını almağa kömək edir. İkincisi, bu yanaşma müzakirəni informasiya texnologiyaları və ya informasiya təhlükəsizliyi çərçivəsindən kənara çıxararaq kiberdavamlılığın uzunmüddətli strateji planlamanın ayrılmaz hissəsi olduğunu tanıyır.

Holistik kiberdavamlılıq yanaşmasının təşviqi təşkilatlar daxilində davamlı strateji dialoqu tələb edir və bu dialoq həm texnoloji, həm də strateji liderləri əhatə etməlidir. Bu yanaşma, "kibertibb" (cybermedicine) yanaşmasına bənzəyərək hazırlığı artırır, təkrarlanan işləri minimuma endirir və nəticədə effektivliyi yüksəldir. Əksinə, ənənəvi təhlükəsizlik tədbirləri tez-tez ikili (binary) yanaşma kimi qəbul edilir; ya sistem təhlükəsizdir, ya da deyil, və adətən icazəsiz istifadəçilərin şəbəkə sisteminə girişinin qarşısını almağa yönəlmiş məhdud texniki funksiyalarla məhdudlaşır.

Kibertəhlükəsizliyin ən çətin aspekti isə naməlum risklərlə üzləşməkdir. ABŞ-ın sabiq Müdafiə Naziri Donald Rumsfeld bunu 2002-ci ildə ustalıqla ifadə etmiş, "məlum məlumlar" (known knowns), "məlum olmayan məlumlar" (known unknowns) və ən çətin kateqoriya olan "naməlum naməlumlar"

(unknown unknowns) arasındakı fərqi vurğulamışdır. Bu kateqoriya təşkilatların əvvəlcədən hazırlıq görmədiyi və proqnozlaşdıra bilmədiyi təhdidləri əhatə edir.

Yeni texnologiyalar ənənəvi yanaşmalardan fərqli imkanlar təqdim edir və sistemləri ciddi təhdidlərdən qorumağa imkan verir. Bu texnologiyalar təşkilat və istifadəçilərin normal davranışını öyrənərək anomaliyaları və potensial riskləri aşkarlayır. Ənənəvi qayda- və imza-əsaslı metodlardan fərqli olaraq, bu texnologiyalar yeni yaranan anomaliyaları və təhdidləri müəyyən edə bilir və naməlum təhlükələr qarşısında adaptiv müdafiə təmin edir, o cümlədən daxili təhlükələr və qabaqcıl kiberhücumlar.

Avropa İttifaqının Kiber Sürətli Cavab Qruplarının (CRRT) inkişafı artıq son mərhələlərinə yaxınlaşır. Layihədə iştirak edən Aİ üzv dövlətlərinin nümayəndələri geniş müzakirələr aparmış, ideyalarını paylaşmış və ortaq bir kiber alətlər dəstəsi üçün planlar hazırlamışdır. Bu alətlər dəsti iştirakçı ölkələrə əsas kibermüdafiə və hadisə idarəetmə qabiliyyətlərini təmin edəcək. Müzakirələr iştirakçıların fərdi ehtiyaclarını və ümumi paylaşılmış vizyonu əhatə etmiş, maliyyələşdirmə mexanizmləri və geniş inkişaf planları müəyyən edilmişdir. Alətlər dəsti CRRT layihəsinin uzunmüddətli uğurunu təmin edən əsas element kimi xidmət edəcəkdir.

Gələcək tədqiqatlar kiberdavamlılığın çevik və effektiv təmin olunması üçün informasiya təhlükəsizliyi sistemlərində səmərəli proseslərin yaradılmasını və tətbiqini araşdıracaq. Bu davamlılıq, sistemin daxili və xarici mühitində tez-tez qarşıya çıxan və proqnozlaşdırılması mümkün olmayan "naməlum naməlumlar" ilə mübarizə aparmaq məqsədini daşıyır. Sürətli Cavab Qrupu (Rapid Response Team) ilkin addım kimi yaradıldıqdan sonra gələcək tədqiqatlar mühüm kiber hadisələrə qarşı qarşılıqlı yardım və əməkdaşlıq imkanlarının formalaşdırılmasına yönələcək. Bu səylər məlumat mübadiləsi, birgə təlimlər, qarşılıqlı əməliyyat dəstəyi və ortaq bacarıqların inkişafını əhatə edəcək.

Əsas olaraq, kiberdavamlılığın inkişafı təhdidlərin davamlı olaraq dəyişdiyi və genişləndiyi mühitdə kritik əhəmiyyət daşıyır. Bu, kiber riskləri təşkilatların geniş strateji məqsədlərinin ayrılmaz elementi kimi qəbul edən, dinamik və adaptiv yanaşmanı tələb edir və beləliklə, qarşılıqlı əlaqəli rəqəmsal dünyada naməlum çağırışlara qarşı proaktiv və əməkdaşlıq yönümlü mövqe formalaşdırır.

NƏTİCƏ

Bu məqalə müasir mürəkkəb rəqəmsal mühitdə yaranan təhlükəsizlik risklərinə qarşı kiberdavamlılığın əldə olunması üçün tələb olunan strategiyalar, proseslər və mexanizmləri araşdırmışdır. Kiberdavamlılıq sahəsində biz informasiya təhlükəsizliyi və kibertəhlükəsizlik aspektlərini əhatə edən innovativ Konseptual Kiberdavamlılıq Modelini təqdim etmişik. Davam edən tədqiqatlarımız kibertəhlükəsizlik informasiya sistemlərinə çevik xüsusiyyətlər qazandıracaq səmərəli və effektiv proseslərin inkişafına yönəlmişdir; bu sistemlər unudulmaz və proqnozlaşdırılması mümkün olmayan hadisələrə, yəni "naməlum naməlumlar"a həm daxili, həm də xarici mühitdə adaptiv, məlumatlı, çevik və məhsuldar şəkildə reaksiya verə biləcək.

Bu yeni konseptual modelin hazırlanması zamanı Avropa İttifaqının Kiber Sürətli Cavab Qrupları (CRRT) və Kibertəhlükəsizlikdə Qarşılıqlı Yardım təşəbbüsünün yaradılması və həyata keçirilməsi ətraflı izah edilmişdir. Beləliklə, Aİ səviyyəsində kibertəhlükəsizlik və kibermüdafiəyə yeni, qabaqcıl bir yanaşma təqdim olunmuşdur.

Bu təşəbbüs Kiberdavamlılıq Modelinin daha geniş kontekstinə yerləşdirilmiş və sistemin bütün səviyyələrində müxtəlif iştirakçıların ümumi məqsədə çatmaqda oynadığı kritik rollar vurğulanmışdır.

Gələcək tədqiqatlar fərdi, şəbəkə və təşkilati kibertəhlükəsizlik idarəetməsi sahələrinə yönələcəkdir. Kiberdavamlılığın əsas Konseptual Modeli xüsusi əhəmiyyət kəsb edir, çünki bu model biliklərin inteqrasiyasına xidmət edir və nəticədə kibertəhlükəsizlik və kibermüdafiə proseslərinin səmərəliliyini və effektivliyini artırır. Məqsəd "naməlum naməlumlar"ın (unknown unknowns) yayılma səviyyəsini azaltmaq və onları tədricən "məlum olmayan məlumlar"a (known unknowns) və "məlum məlumlar"a (known knowns) çevirməkdir. Bu təkamül trayektoriyası daim dəyişən kiber təhlükə mənzərəsində hərəkət etmək qabiliyyətimizi inkişaf etdirmək üçün vacibdir.

ƏDƏBİYYAT

[1] F. Nonino and G. Palombi, "Understanding the management of cyber resilient systems," *Computers & Industrial Engineering*, vol. 149, p. 106829, 2020.

[2] M. Amini and Z. Bozorgasl, "A game theory method to cyber-threat information sharing in cloud computing technology," *International Journal of Computer Science and Engineering Research*, 2023.

[3] V. Greiman, "Known unknowns: The inevitability of cyber attacks," in *Proc. European Conf. Cyber Warfare and Security*, Jun. 2023.

The Concept of Cyber Resilience and Its Role in Ensuring Cyber Sovereignty

Rauf İsmayılzadeh

The Academy of the State Security Service of the Republic of Azerbaijan named after Heydar Aliyev, Baku, Azerbaijan

Abstact— Cybersecurity is a field closely related to the security of information and operational technologies, encompassing various techniques and concepts. Its main characteristic is the possibility of employing offensive IT strategies against an adversary. However, the broad and imprecise use of the term often equates it with information security or IT security, leading to misunderstandings and obscuring important distinctions. The article proposes that the term "cybersecurity" should be limited to practices focused on defense within IT environments. The study analyzes the relationship between cybersecurity, cyber defense, and cyber resilience, introduces a new conceptual framework, and examines the role of CRRT.

Keywords– Cyber Resilience; Cybersecurity; Cyber Defense; Rapid Response Teams.