Elektron dövlətdə informasiya müharibəsinin bəzi modelləri haqqında

İradə Ələkbərova
AMEA-nın İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
airada.09@gmail.com

Xülasə– Məqalədə informasiya müharibəsi ilə əlaqədar müəyyən terminlər şərh olunur, e-dövlətə qarşı informasiya müharibəsinin məqsəd və hədəfləri göstərilir. İnformasiya müharibəsidə istifadə olunması nəzərdə tutulan bəzi modellər analiz olunur.

Açar sözlər - e-dövlət, informasiya hücumu, kritik infrastruktur, informasiya müharibəsi modeli, psixoloji təsir, kibermüharibə

I. GIRIŞ

E-dövlət müasir informasiya kommunikasiya texnologiyalarından (İKT) istifadəyə əsaslanan yeni dövlət tipidir. E-dövlətin formalaşmasında əsas şərt kimi vətəndaşların özünəxidmət imkanlarının dəstəklənməsi və genişlənməsi, seçicilərin dövlətin idarə olunmasında iştirakının təmin olunması, onların coğrafi məhdudiyyətləri ilə əlaqədar yarana biləcək problemlərin aradan qaldırılmasıdır ki, bu şərtləri müasir İKT vasitəsi ilə təmin etmək mümkündür. Üstünlüyü münasibətlərdə şəffaflıq, yüksək rahatlıq, korrupsiya hallarının qarşısının alınması və xərclərin azalmasıdır.

İnformasiya cəmiyyətinin (İC) formalaşması, e-dövlət quruculuğunda istifadəsi nəzərdə tutulan layihələrin çoxalması və təkmilləşdirilməsi nəticəsində dövlət strukturlarına aid kompüter şəbəkələrinin və virtual məkanın təhlükəsizliyinə tələbat çoxalmaqdadır. Müxtəlif illərdə İP protokolunun universallığından ortaya çıxan imkanlar, veb-texnologiyalarının inkişafı və onlardan geniş istifadə nəticəsində real təhlükələr artmışdır. Bu baxımdan e-dövlətin idarə olunmasında əsas şərt onun təhlükəsizliyidir.

II. İNFORMASIYA MÜHARIBƏSI ILƏ BAĞLI ANLAYIŞLAR

E-dövlətin formalaşması və informasiyanın rolunun cəmiyyətdə həddən artıq artması nəticəsində "informasiya hücumu" (*information attaks*), "informasiya qarşıdurması" (*information confrontation*) və "informasiya müharibəsi" (*information warfare*) terminləri insanların gündəlik həyatında tez-tez istifadə olunmaqdadır [1].

İnformasiya qarşıdurması – tərəflərin xüsusi metodlardan, informasiya resurslarına təsir üsulları və vasitələrindən istifadə etməklə informasiya resurslarının məhvinə və ya nəzarətdə saxlanmasına yönəlmiş informasiya əməliyyatıdır [2]. *İnformasiya hücumu* isə icazə olmadan istənilən formada informasiyanın köçürülməsi, dəyişdirilməsi və məhvinə, həmçinin, proqram təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatdır [3]. İnformasiya müharibəsi isə özündə informasiya hücumu və qarşıdurması kimi əməliyyatları birləşdirən daha təhlükəli informasiya təsiri formasıdır.

İnformasiya müharibəsi qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi, hərbi potensialını ələ keçirmək uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir. İnformasiya müharibəsində informasiya həm silah, həm də məqsəddir [4].

E-dövlətə qarşı informasiya müharibəsindən danışarkən yalnız texniki vasitələrin məhvi və nəzarətdə saxlanması deyil, eyni zamanda insan faktoru da nəzərə alınmalıdır. Müasir informasiya müharibəsi texnologiyalarının yaranması, inkişafı və geniş tətbiqinin müxtəlif izahları var [5]:

1. Hesablama texnikası və kommunikasiya vasitələrinin sürətli inkişafı, şəbəkə texnologiyasının təkmilləş-dirilməsi cəmiyyətdə əsas resurs kimi informasiyanın rolunun artmasına səbəb oldu.
2. Effektivliyinə görə informasiya maddi resurslardan daha yuxarıda dayandı. Elmi-texniki nailiyyətlər hərbi sahədə istifadə edilən ənənəvi silahlarla yanaşı bir sıra İKT vasitələrinin kütləvi istehsalına və informasiya təhlükəsizliyinin təmini üçün geniş istifadəsinə şərait yaratdı.
3. İnsanların beyinlərinin və davranışlarının öyrənilməsində əldə edilən nailiyyətlər insanlara müxtəlif istiqamətlərdə psixo-fizioloji təsirlərin yollarını və vasitələrini daha yaxşı başa düşməyə imkan verdi.

"İnformasiya müharibəsi" terminini ilk dəfə 1976-cı ildə amerikalı mütəxəssis Tomas Rona (*Thomas Rona*) "Boeing" kompaniyası üçün hazırladığı "Silah sistemləri və informasiya müharibəsi" adlandırdığı hesabatında istifadə etmişdir. Rona hesabatında sübut etmişdir ki, son illərdə informasiya infrastrukturu dövlətin iqtisadiyyatının əsas komponentinə çevrilmişdir [5].

İnformasiya müharibəsinin ilk tədqiqatçılarından biri, ABŞ-ın Milli Müdafiə Universitetinin əməkdaşı Martin Libiki (*Martin Libicki*) 1995-ci ildə yazdığı "İnformasiya müharibəsi nədir?" məqaləsində informasiya müharibəsi texnologiyalarının təsnifatını vermiş və göstərilmişdir ki, son dövrlərdə İKT-nin inkişafı nəticəsində artıq informasiya müharibəsində yalnız psixoloji deyil, əsasən iqtisadi və hərbi aspektlərə üstünlük verilir İnformasiya müharibəsinin mərhələləri [6]:

– *Məqsədin təyin edilməsi.* İnformasiya müharibəsi nə üçün lazımdır və nəticədə nə əldə ediləcəyi gözlənilir.

- *Strategiyanın təyin edilməsi.* Burada İKT-nin dörd baza kompanenti nəzərə alınmalıdır: informasiyanın hazırlanması, informasiyanın yönələcəyi kommunikasiya kanalının təyin edilməsi, informasiyanın təsiri altına düşəcək auditoriyanın müəyyənləşdirilməsi, informasiya müharibəsi metodunun seçilməsi.
- *Taktiki fəaliyyət planının hazırlanması*.

III. E-DÖVLƏTƏ QARŞI İNFORMASİYA MÜHARİBƏSİNDƏ MƏQSƏD VƏ HƏDƏFLƏR

1993-cü ildə Con Arkuilla (*John Arquilla*) və Devid Ronfeldt (*David Ronfeldt*) tərəfindən "Kibermüharibə gəlir!" (*Cyber War Is Coming*!) məqaləsində "Şəbəkə müharibəsi" (*Network War*) termini istifadə edilmişdir. Məqalədə müəlliflər kibernetik və şəbəkə müharibəsi konsepsiyalarını (*Network Centric Warfare, NCW*) irəli sürməklə müasir dövrdə informasiya müharibəsinin ənənəvi müharibədən daha ciddi problemlər yaratmaq imkanına malik olduğunu göstərdilər [7].

Konsepsiyada informasiya müharibəsinin əsas məqsədi kimi aşağıdakılar göstərilirdi:

1. Öz informasiyasını və informasiya sistemlərini qorumaqla qarşı tərəfin informasiya məkanına nəzarət;
2. Qarşı tərəfin informasiyasını nəzarətdə saxlamaqla informasiya hücumuna başlamaq (qarşı tərəfin iqtisadiyyatını ələ keçirmək və ya məhv etmək);
3. İnformasiyadan istifadə etməklə özünün ümumi güc potensialını yüksəltmək;
4. İnformasiya-psixoloji təsir vasitələrindən istifadə etməklə qarşı tərəfə psixoloji təsir.

Dövlətin iqtisadi və elmi-texniki siyasətinin bir istiqaməti kimi milli informasiya təhlükəsizliyi məsələsi həll edilməlidir. İnformasiya təhlükəsizliyinin təmin edilməsi sistematik, kompleks yanaşma tələb edir. Bu sahədə əlaqədar qurumlar tərəfindən konseptual, təşkilati, elmi-metodoloji, qanunvericilik, maddi-texniki əsasların yaradılması üzrə işlərin aparılması müasir dövrün ən vacib məsələlərindəndir. İnformasiya müharibəsinin fundamental paradiqması və ya dörd strategiyası aşağıdakı informasiya əməliyyatlarıdır [8]:

1. İnformasiyanın təqdimatından imtina (Denial of Information, DoI) / dağıdılma və ya məhv edilmə Degradation or Destruction, DoD).
2. Aldatma və mimikriya (Deception and Mimicry) / Corrupsiya (Corruption) – bilərəkdən yanlışlığa yönəldən informasiyanın ötürülməsi əməliyyatı.
3. Ayırma və məhv etmə (Disruption and Destruction) / imtina etmə (Denial) – daxildən disfunksiya yaradan və informasiyanın məhvinə yönəlmiş əməliyyat.
4. Təxribatçı əməliyyatlar (SUBversion) / imtina etmə (Denial) – qarşı tərəfin sistemində destruktiv prosesə səbəb olan informasiyanın daxil edilməsi əməliyyatı.

E-dövlətdə informasiya müharibəsi zamanı müşahidə olunan əsas informasiya əməliyyatları şəbəkənin normal fəaliyyətinə yönəlmiş müxtəlif hücumlardır.

E-dövlətdə informasiya hücumu dedikdə elektron sənədlərin dəyişdirilməsi, məhvi və ya serverlərdəki proqram təminatlarına, verilənlərin saxlandığı texniki qurğulara, ötürücü vasitələrə və şəbəkəyə yönəlmiş informasiya əməliyyatları nəzərdə tutulur [9]. E-dövlətdə informasiya müharibəsinin əhatə etdiyi sahələr aşağıdakılardır:

- Dövlətin maddi rifahını təmin edən kritik infrastruktur.
- İqtisadi sahələr.
- Vətəndaşların şəxsi məlumatları: şifrələr, bank hesabları və s.
- İnternet şəbəkəsi.

İnternetdə informasiya qarşıdurması vasitələrinin universallığı, gizliliyi, çoxvariantlılığı, təsirin radikallığı, təminatın kifayət qədər zaman və məkan seçimi, nəhayət, əlverişli olması onları həddən artıq təhlükəli edir və bu xüsusiyyətlər qlobal şəbəkədə informasiya müharibəsinin gizli aparılması üçün uyğun şərait yaradır.

E-dövlətə qarşı informasiya müharibəsində əsas hədəf kimi kritik infrastrukturlar (*Critical infrastructures*) nəzərdə tutulur. Kritik və ya başqa sözlə həyati əhəmiyyət kəsb edən infrastruktur dedikdə dövlətin, dövlət orqanlarının və vətəndaşların normal fəaliyyətini və rifahını təmin edən əsas infrastrukturlar nəzərdə tutulur. Bu infrastrukturların dağıdılması və ya fəaliyyətlərində pozuntular dövlət strukturlarının və hökumətin işində böyük çətinliklər törədə bilər [10].

Kritik infrastrukturlara aiddir: informasiya və kommunikasiya (*Information and Communications*), bank və maliyyə (*Banking and Finance*), enerji sahələri (elektrik enerjisi, neft və qaz), fiziki paylanma (*Physical Distribution*) və insan kapitalı (*Human Services*) [11].

İnformasiya müharibəsinin əhatə etdiyi sahələri nəzərə alaraq deyə bilərik ki, e-dövlətdə informasiya müharibəsi idarəetmə və qərarların qəbulu sistemlərinə (*Command & Control Warfare, C2W*), həmçinin, kompüter şəbəkələrinə və informasiya sistemlərinə (*Computer Network Attack, CNA*) qarşı yönəlmiş informasiya əməliyyatları ilə həyata keçirilir. İdarəetmə və qərarların qəbulu sistemlərinə destruktiv təsir zamanı qərarların qəbulunda iştirak edən məsul şəxslərə və personala qarşı psixoloji əməliyyatlar da (*Psychological Operations, PSYOP*) nəzərə alınmalıdır.

E-dövlətə qarşı informasiya müharibəsində aşağıdakı əsas üç istiqamətlər nəzərə alınmalıdır:

- Elektron hücum (*electronic attack, EA*),
- Elektron müdafiə (*electronic protect, EP*)
- Müharibəyə elekron dəstək (*electronic warfare support, ES*)

E-dövlətə qarşı informasiya müharibəsində bu istiqamətlərin hər biri üçün ayrılıqda metodlar işlənməlidir: elektron hücum metodları, elektron müdafiə metodları və müharibəyə elekron dəstək metodları.

İnformasiya müharibəsi texnologiyalarının analizi nəticəsində məlum olmuşdur ki, e-dövlətdə informasiya müharibəsi metodlarına aiddir: elektron müharibə (*Electronic Warfare),* psixoloji müharibə *(Psychological Warfare),* internet şəbəkəsində kəşfiyyat müharibəsi (*Information Based Warfare*), haker müharibəsi (*Hacker Warfare*) və kibermüharibə (*Cyberwar*) [4, 8, 9].

İnformasiya müharibəsində məqsəd və hədəflərin, müharibə metodlarının araşdırılması e-dövlət quruculuğunda və İC-nin inkişafında informasiya təhlükəsizliyi problemlərinin effektiv həlli üçün vacib məsələlərdəndir. Belə ki, kompüter şəbəkələrində informasiya əməliyyatları ilə əlaqədar pozuntuların təyin edilməsində, konkret vəziyyət üçün daha çox ehtimal olunan təhlükələrin təyinində və informasiya təhlükəsizliyi ilə əlaqədar işlərin təşkilində mühüm əhəmiyyətə malikdir.

IV.İNFORMASİYA MÜHARİBƏSİNİN BƏZİ MODELLƏRİ

Valts modeli (*Model Waltz*) informasiya təhlükəsizliyinin əsas 3 aspektinə hücumları nəzərdə tutur: məxfilik, tamlıq və əlyetərlik. Model informasiya müharibəsinin əksər istiqamətlərində istifadə olunur və əhatəlidir [12] (cədvəl 1).

Borden və Kopp tərəfindən işlənmiş **Borden-Kopp modeli** informasiya müharibəsində istifadə olunan 1-ci dərəcəli riyazi modellərdəndir. Şennonun informasiya nəzəriyyəsinə (*Shannon's information theory*) [13] əsaslanmış Borden-Kopp modeli şəbəkə ilə ötürülən informasiyanın sayını təyin edir. Model informasiyanı müvəffəqiyyətlə küylü şəbəkələrlə ötürə bilir. Borden-Kopp modelində küylərdən istifadə etməklə yalnız 4 növ hücum nəzərdə tutulur: deqresiya (*degrade*), korlamaq (*corrupt*), inkar (*deny*) və istismar (*exploit*). İnkar etmək dedikdə birbaşa hücumlarla informasiyanın qarışdırılması və dağıdılması nəzərdə tutulur. Model həmçinin siqnalları ələ keçirərək müxtəlif məqsədlər üçün istifadə edə bilir [14–15].

Modeldə İnformasiya əməliyyatları üçün 4 mərhələ nəzərdə tutulur: informasiyanın toplanması (*collected*), dağıdılması (*moved*), saxlanması (stored) və situasiyanın qiymətləndirilməsi (*situation assessment*) [13].

Hatçinson və Uorren modeli (*Model Hutchinson and Warren*) qarşı tərəfin informasiyasının məhvinə, oğurlanmasına və dağıdılmasına yönəlmişdir [16]. Model Borden-Kopp modelinə oxşardır. Fərq yalnız ondadır ki, Hatçinson və Uorren modeli daha geniş imkanlara malikdir: qarşı tərəfə dəqiq informasiya əldə etmək imkanı verilmir, şəbəkənin normal funksiyası pozulur, qarşı tərəfin malik olduğu informasiya birbaşa və ya dolayı yolla məhv edilir.

Fliger və Fliger modeli (*Model Pfleeger and Pfleeger*) informasiyanın ələ keçirilməsi, qırılması və istismarını nəzərdə tutur. Model digər modellərlə müqayisədə daha sadə görünsə də informasiyanın tamlığı, məxfiliyi və əlyetərliyinə qarşı hücum əməliyyatlarını uğurla yerinə yetirə bilir [17].

USAF (US Air Forsee) modeli Valts tərəfindən təklif edilmişdir. Digər modellər informasiyanın dəyişdirilməsi və korlanması kateqoriyasına daxil olduqları halda USAF modeli spesifik elementlərinə görə digərlərindən fərqlənir. USAF modeli informasiyanın dağıdılması ilə yanaşı kompramat informasiyanın toplanması məsələlərini də həll etmək imkanına malikdir [18].

Cədvəl 1. İnformasiya müharibəsi üzrə bəzi modellərin müqayisəsi

İnf. müharibəsi modelləri	İnformasiya əməliyyatları	Nəticə
Model Waltz (1998)	Tamlığa təsir Məxfiliyin və əlyetərliliyin pozulması	İnformasiya korlanır
Borden-Kopp model (1999)	Keyfiyyətə təsir Deqradasiya İmtina	İnformasiya korlanır
Model Hutchinson and Warren (2001)	İnformasiyanın dəyişdirilməsi İmtina Manipulyasiya	İnformasiya oğurlanır
Pfleeger and Pfleeger (2003)	İnformasiyanın ötürülməsinə mane olmaq	İnformasiya qırılır
USAF (1998)	İnformasiyanın dağıdılması İmtina Aldatmaq	Kompramat informasiya toplanır

İnformasiya müharibəsinin ümumi modeli (*General Information Warfare models*) 2009-cu ildə Ventre tərəfindən təklif olunmuşdur. Ventre bildirir ki, kompüter şəbəkələri və İnternetdə baş verən informasiya müharibələrinin əsas səbəbi dünyada siyasi gərginliyin artmasıdır. Təklif olunan model kiberhücumlar üçün nəzərdə tutulsa da istənilən insident üçün istifadə oluna bilər. Modeldən dövlətin vacib infrastrukturlarında və şəbəkələrində istifadə etmək mümkündür. Model hədəflərə hücum informasiyanın dəyişdirilməsinə və yeni informasiyanın yaradılmasına əsaslanmışdır ki, bu da əsasən vətəndaşlara psixoloji təsir ilə nəticələnir [19].

Digər psixoloji hücum **məlumatlar axını modeli** (*The Message Flow Model*) adlanır. Koks tərəfindən təklif olunan model vətəndaşların davranışlarının dəyişdirilməsinə yönəlmişdir. Psixoloji təsir zamanı insanlarda qorxu və gərginlik yaradır. Model insanların reaksiyasına görə ötürülən məlumatları qiymətləndirir [20]

Dövri həyat modeli (*Life Cycle Model*) müxtəlif insidentlərin təsvirini verir və informasiya müharibəsinin müxtəlif formalarına eyni zamanda tətbiq oluna bilir.

Metodların fərqliliyi modelin tətbiqinə mane olmur. Məsələn, psixoloji təsir və radioelektron müharibə [21].

E-dövlətin effektli idarə olunması üçün hökumət siyasi, hüquqi və diplomatiya sahələrində istifadə olunan informasiya resursları və şəbəkənin təhlükəsizliyini təmin etməlidir. Araşdırmalar göstərdi ki, e-dövlətdə informasiya müharibəsi ilə bağlı problemləri yalnız informasiya sisteminin və ya kompüter şəbəkəsinin təhlükəsizliyini gücləndirməklə həll etmək mümkün deyil. E-dövlət quruculuğunda istənilən informasiya şəbəkəsinin layihələndirilməsini həyata keçirərkən, artıq sabah onun informasiya əməliyyatları meydanına çevriləcəyini nəzərə almaq lazımdır. İnformasiya təcavüzünün qarşısını almaq, informasiya qarşıdurmasında uğur əldə etmək üçün isə ilk növbədə informasiya hücumlarında istifadə olunan informasiya müharibəsi modellərini öyrənmək, onlara qarşı qabaqlayıcı tədbirlər görmək lazımdır.

V. NƏTİCƏ

Tədqiq edilən informasiya müharibəsi modellərinin tətbiqi yüksək səviyyəli informasiya əməliyyatlarına aid olduğundan və yönəldici xarakterlərinə görə ən yüksək infrastrukturun müdafiəsində istifadə edilə bilər. İnformasiya müharibəsi hədəfləri ilə kritik infrastruktur eyni deyil və bu səbəbdən informasiya müharibəsi modelinin bütün mümkün ssenarilərdə tətbiqini gözləmək düzgün deyil. Hər bir model ilk növbədə müəyyən konseptual səviyyədə, mühütə uyğun insidentlər üçün tətbiq oluna bilər.

İnformasiya müharibəsinin fundamental modellərinin bəzilərinin analizi və müqayisəsi e-dövlətdə kritik infrastrukturun müdafiəsində mühüm rol oynaya bilərlər.

ƏDƏBİYYAT

[1] Расторгуев С.П. Информационная война // Москва, Радио и связь, 1998. с. 35–37.

[2] Абдурахманов М.И., Баришполец В.А., Баришполец Д.В., Манилов В.Л. Геополитика, международная и национальная безопасность, Словарь-справочник. Под общей редакцией В.Л. Манилова, 1999, «Пробель», Москва, с. 127–130

[3] Ələkbərova İ.Y. İnformasiya müharibəsi texnologiyaları, “İnformasiya texnologiyaları” nəşriyyatı, Bakı, 2012, 108 səh.

[4] Thomas P. Rona, “Weapon Systems and Information War” // Boeing Aerospace Co., Seattle, WA, 1976, pp. 14

[5] Ələkbərova İ.Y. İnformasiya müharibəsi texnologiyalarının analizi və təsnifatı // İnformasiya cəmiyyəti problemləri, 2010, Bakı, №2, səh. 80–91.

[6] Libicki M., What is Information Warfare? // National Defense University. ACIS, 1995, pp. 3

[7] Arguilla J., Ronfeldt D., Cyberwar is coming! // Comparative Strategy, 1521-0448, Volume 12, Issue 2, 1993, pp. 141–165

[8] Kopp C. A Fundamental Paradigm of Infowar, 2005, http://www.ausairpower.net/OSR-0200.html

[9] Алекперова И.Я., Comparative analysis of information attacks in Internet // журнал «Информационные технологии и компьютерная инженерия», Украина, Винница, №3 (19), 2010, стр. 81–87.

[10] Moteff, J & Parfomack, P. Critical infrastructure and key assets: Definition and identification. Washington, DC: Congressional Research Service, 2004, 4.

[11] Ware, WH. The cyber posture of the national information infrastructure. Santa Monica, CA: RAND Institute, 1998, 4.

[12] Waltz op. cit., p. 23.

[13] Shannon C. E. A Mathematical Theory of Communication // The Bell System Technical Journal, 1948, vol. 27, no 3, pp. 379–423.

[14] Borden A. What is information warfare // Air and Spase Power, Online journal, 1999, http://www.au.af.mil/info-ops/infowar.htm

[15] Kopp C. The four strategies of information warfare and their applications // IO Journal, 2010, vol. 1, no 4, pp. 28-33/

[16] Hutchinson W., Warren M. The law and cyber terrorism // Journal of information warfare, 2003, vol. 2, no. 2, pp. 27-32.

[17] Pfeeger P., Pfleeger S. Security in computing, 3rd edition. Upper Saddle River, NJ: Prentice Hall, 2003, pp. 26–36.

[18] Brett N., Manoj S. M. Relevance of information warfare models to critical infrastructure protection // Journal of Military Studies, 2011, vol. 39, no 2, pp. 99–122.

[19] Ventre D. Information Warfare, Wiley-ISTE, 2009, 320 p.

[20] Cox L. V. Planning for psychological operations a proposal. The Research Department. Air Command and Staff College, 1997, 91 p.

[21] http://www.au.af.mil/au/awc/awcgate/acsc/97-0363.pdf

[22] Brett N., Manoj S. M. The Information Warfare Life Cycle Model // Journal of Information Management, 2011, vol. 13, no 1, pp. 11–20.