UOT 004.9:351

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

KİBERQOŞUNLAR: FUNKSIYALARI, SILAHLARI VƏ KADR POTENSİALI

Ölkələr arasındakı münaqişələr kiberfəzaya da keçir və virtual məkanda həm sülh, həm də müharibə dövründə əməliyyatlar aparmaq üçün xüsusi qoşun növləri – kiberqoşunlar yaradılmağa başlayır. Bir sıra ölkələrdə milli informasiya təhlükəsizliyini təmin etmək üçün kiberqoşunlar mövcuddur və ya yaxın illərdə yaradılması planlaşdırılır. Bu işdə kiberqoşunların formalaşdırılması problemləri tədqiq edilir. Kiberqoşunların yaradılmasının əsas aspektləri, kiberqoşunların məqsədləri və funksiyaları, kiberkomandanlığın struktur-təşkilati modelləri araşdırılır, kiberqoşunların silah arsenalı və kadr potensialı, inkişaf etmiş ölkələrin bu sahədə təcrübəsi analiz edilir. Kiberqoşunların və kibertəhlükəsizliklə əlaqəli digər dövlət təşkilatlarının fəaliyyətinin koordinasiyası və beynəlxalq əməkdaşlıq məsələləri də müzakirə edilir.

Açar sözlər: *informasiya müharibəsi; kibermüharibə; kibermüdafiə; kiberqoşun; kibersilah; kiberkomandanlıq.*

Giriş

Qloballaşmanın hazırki mərhələsində dövlətlərarası ziddiyyətlərin və münaqişələrin fəal şəkildə informasiya fəzasına keçirilməsi, informasiya qarşıdurmalarının yaradılması və idarə olunması, genişmiqyaslı informasiya müharibələrinin aparılması müşahidə olunur. Qlobal informasiya fəzasının bir hissəsi olan kiberfəza da sürətlə hərbiləşdirilir, hərbi və mülki hədəflərə kiberhücumların sayı kəskin surətdə artır və kibermüharibələr müasir müharibə arsenalına daxil olur [1, 2]. 2007-2008-ci illərdə ilk dövlətlərarası kiçikmiqyaslı kibermüharibələr (Estoniya və Gürcüstana qarşı) baş vermişdir [3, 4].

Ölkənin hərbi, iqtisadi, diplomatik, siyasi, mədəni və bioloji suverenliyi ilə yanaşı informasiya suverenliyinin təmin edilməsi də milli təhlükəsizlik məsələsinə çevrilir [5]. Bəzi dövlətlər artıq informasiya fəzasını (hava, quru, dəniz və kosmosla yanaşı) xüsusi döyüş meydanı hesab edirlər. Dövlətlərin kibermüharibə təhdidlərinə qarşı gördüyü tədbirlərdən biri də xüsusi qoşun növünün – kiberqoşunların yaradılmasıdır [6]. Kiberqoşunlar silahlı qüvvələrin tərkibində hərbi kibertəhdidlərlə mübarizə aparmaq üçün formalaşdırılır.

Kiberqoşunların yaradılmasına 2000-ci illərdə ABŞ-da başlanılması məlumdur və bir çox ölkə yaxın illərdə fəaliyyətə tam hazır kiberqoşunlar formalaşdırmağı planlaşdırır [7]. Bəzi məlumatlara görə, dünyanın 140 ölkəsində kiberqoşunların yaradılması və ya genişləndirilməsi təşəbbüsləri vardır. Onların bir çoxu hücum xarakterlidir. Hərbi baxımdan kibermüharibələr cəlbedici və şirniklərdiricidir: öz əsgərlərini risk altında qoymur; təcavüzkarın izinə tam əminliklə düşmək mümkün deyil; hücumun mənbəyi saxtalaşdırıla bilər və şübhə yeri qalmadan müəyyənləşdirmək mümkün olmur [7].

Bu işdə kiberqoşunların formalaşdırılması problemləri analiz edilir, inkişaf etmiş ölkələrin və beynəlxalq hərbi təşkilatların bu sahədə təcrübəsi açıq məlumatlar əsasında araşdırılır. Kiberqoşunların yaradılmasının əsas aspektləri, kiberqoşunların məqsədləri və funksiyaları, kiberkomandanlığın struktur-təşkilati modelləri, kiberqoşunların silah arsenalı və kadr potensialı analiz edilir. Ölkənin kiberfəzada suverenliyini mümkün qədər tam təmin etmək üçün kiberqoşunların formalaşdırılması və inkişafı sahəsində beynəlxalq əməkdaşlıq məsələləri müzakirə edilir.

Əsas anlayışlar və terminlər

Kiberqoşunların məqsəd və funksiyalarını dəqiq müəyyən etmək üçün bir sıra anlayış və terminlərin əvvəlcədən razılaşdırılması zəruridir (“termin” anlayışı latınca “term” – sərhəd, hədd

sözündən yaranmışdır). Məqalənin qalan hissəsində aşağıdakı terminlər sistemindən istifadə ediləcək [8]:

Kibersilah – informasiya texnologiyalarına əsaslanan digər sistemlərin strukturuna və əməliyyatlarına ziyan vurmaq üçün yaradılmış, informasiya texnologiyalarına əsaslanan sistem (aparat, proqram təminatı və kommunikasiya mühitindən ibarət olur).

Kiberinsident – informasiya sisteminin strukturunda və əməliyyatlarında yolverilməz kənaraçıxmalara səbəb olan (və ya ola bilən) hadisələrdir. Kiberinsidentlər qəsdən və ya təsadüfən törədilə bilər. Kiberinsidentlərin aktorları (tərəfləri) fərdlər, fərd qrupları, şirkətlər və ya dövlətlər ola bilər. Bir-birinə kibersilahlarla hücum edən tərəflərin bütün mümkün kombinasiyaları müxtəlif ssenariləri əks etdirir, onları təsirindən asılı olaraq kibercinayət əməli, sənaye casusluğu, kiberterrorizm, kibermünaqişə və (kiber)müharibə adlandırmaq olar.

Kiberhücum – kiberinsident yaratmaq üçün informasiya sistemlərinə qarşı kibersilahın və ya kibersilah kimi istifadə edilə bilən sistemin qəsdən istifadəsidir.

Kibercasusluq – hədəf sistemin konfidensiallığını pozmaq üçün kiberhücumların istifadəsidir.

Kibermünaqişə – siyasi məqsədlərə nail olmaq üçün kiberhücumların istifadəsidir (hədəf sistemlərin tamlığına və əlyetərliliyinə qarşı yönəlmiş hücumlar daxil olmalıdır). Burada kibermünaqişə anlayışı dar mənada işlədilir. Geniş mənada kibermünaqişə dedikdə, ümumiyyətlə, üstünlük qazanmaq üçün kiberfəzadan istifadə edilməsi nəzərdə tutulur.

Kibermünaqişə gedişində üç əsas əməliyyat: çəkindirmə, qarşısını alma və rəqəmsal meydanda münaqişələrin həlli nəzərdə tutulur. Lakin bəzi ölkələr virtual fəzada baş verən münaqişələrə adi müharibələrdə qəbul edilmiş metodlarla adekvat cavab verilməsi variantını da istisna etmirlər.

Kibermüharibə – ölkələr arasında kibermünaqişədir, yəni kibermüharibə – kiberfəzada hərbi əməliyyatlardır. Buraya həm hərbçilərin dövlətin silahlı qüvvələrinə qarşı döyüş hücumları (məsələn, düşmənin kritik vacib rabitə kanallarının sıradan çıxarılması), həm də mülki əhaliyə qarşı olan hücumlar daxildir. Kibermüharibə anlayışı 2007-ci ilin yazında Estoniyada ABŞ səfirliyinin, Estoniya nazirliklərinin, banklarının, KİV-in serverlərinə olan hücumlardan sonra geniş işlənilməyə başlandı [3].

Qeyd edək ki, "kibermüharibə" daha geniş anlayış olan "informasiya müharibəsi" anlayışının, "kiberqoşun" isə "informasiya qoşunları" anlayışının tərkibinə daxildir.

İnformasiya müharibəsi qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi və hərbi potensialını ələ keçirmək, ictimai şüura informasiya təsiri göstərməklə insanların davranışlarını dəyişmək uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir [9]. Martın Libiki informasiya müharibəsinin yeddi formasını göstərir [10]: (1) komanda-nəzarət kanallarına yönəlmiş informasiya hücumları; (2) kəşfiyyat müharibəsi; (3) elektron kommunikasiya vasitələrinə qarşı müharibə; (4) psixoloji müharibə; (5) haker müharibəsi – qarşı tərəfin mülki obyektlərinə yönəlmiş virtual diversiya əməliyyatları; (6) iqtisadi informasiya müharibəsi; (7) kibermüharibə – sistemin fiziki göstəricilərinə, şəbəkənin və kompüterin normal işini təmin edən obyektlərə yönəlmiş əməliyyatdır.

Kiçik komandalardan kiberqoşunlara doğru

Kiberqoşunların inkişafı üçün zəmin kiçik komandaların - haker komandalarının, "qırmızı" və "mavi" komandaların və *CERT* komandalarının (*Computer Emergency Response Team*) meydana çıxması və inkişafı ilə hazırlanmışdır [11]. Hərbçilər informasiya təhlükəsizliyi məsələlərinin həlli üçün bu komandaların xidmətlərindən istifadə edirdilər. Problemlər mürəkkəbləşdikcə və miqyası böyüdükcə kiberqoşunların yaradılması məsələsi gündəmə gəldi.

Kiberqoşunların statusu hələlik tam müəyyən edilməyib. Çox vaxt onlar mövcud qoşun növlərindən heç birinə aid edilmirlər və onları əsas vəzifəsi kibertəhlükələrlə mübarizə

aparmaqdan ibarət olan yeni qoşun növü hesab edirlər [5,6]. Kiberqoşunların ayrıca qoşun növü kimi formalaşdırılması prosesləri resurs və kadr təminatının, doktrinal və strateji bazasının yaradılmasını tələb edir. Kiberqoşunların formalaşdırılması üçün daha çox ABŞ Müdafiə Nazirliyinə məxsus *DOTmLPF* (*Doctrine, Organization, Training, Material, Leadership and education, Personnel and Facilities* − Doktrina, təşkil, treninq, material, rəhbərlik, təhsil, şəxsi heyət və qurğular) yanaşmasından istifadə edilir [7].

Adətən, ölkələrin kiberqoşunlar sahəsində açıqlanan strategiyaları müdafiə xarakterlidir, kibermünaqişə gedişində üç əsas əməliyyat: çəkindirmə, qarşısını alma və kiberfəzada münaqişələrin həlli nəzərdə tutulur. Lakin bəzi ölkələr kiberhücumlara adi müharibələrdə qəbul edilmiş metodlarla adekvat cavab verilməsi variantını da istisna etmirlər (hücum kiberəməliyyatları üzrə ABŞ Prezidentinin Direktivi – *Presidential Policy Directive* 20) [12].

Kiberqoşunların əsas vəzifəsi – hərbi sistemlərə yönələn kiberhücumlarla mübarizə kimi müəyyən edilir, onlar çox zaman *CERT* qurumları kimi təşkil olunurlar. Lakin fərqli yanaşmalar, fərqli funksiyalar, əməliyyatlar (hətta kibercasusluq da daxil olmaqla) haqqında məlumatlar da vardır. Məsələn, ABŞ kiberqoşunlarının əsas vəzifəsi bu ölkənin hərbi kompüter şəbəkələrinin idarə edilməsi və müdafiəsi, kibermüharibə əməliyyatlarının mərkəzləşdirilmiş qaydada həyata keçirilməsidir.

Müasir hərbi texnika və silahlarda, qoşunların idarə edilməsi sistemlərində informasiya (kompüter) texnologiyaları geniş istifadə edilir. Hərbi texnikada xarici elektronikanın geniş istifadə edilməsi, onlarda gizli əl yerlərinin qoyulması ehtimalı müasir silahların "Axilles" dabanıdır. Kiberqoşunların vəzifələrinə kiberhücumların qarşısının alınması ilə yanaşı, zərərli proqram təminatının aşkarlanması və hərbi avadanlıqda gizli əl yerlərinin axtarılması da daxil ola bilər. Bəzi dövlətlərin kiberqoşunlarının funksiyalarına potensial düşmən qoşunlarının idarə edilməsi sistemlərinin işini tamamilə pozmaq tədbirləri də daxildir.

Kiberqoşunların silah arsenalı

Kiberqoşunların silah arsenalını iki qrupa bölmək olar: adi kibersilahlar və qabaqcıl kibersilahlar.

*Adi kibersilahlar*a kiberhücumların həyata keçirilməsinin həyat tsikli üçün *Martin Lockheed* şirkəti əməkdaşlarının təklif etdiyi kiberzərbə zəncirindəki [13] bütün əməliyyatları yerinə yetirmək üçün nəzərdə tutulmuş haker alətlərini aid etmək olar ki, onların əksəriyyəti İnternetdə əlyetərdir. Bu arsenala hazırda yüzlərlə alət daxildir (məsələn, *BackTrack Linux* paketində 300-dən artıq açıq kodlu təhlükəsizlik aləti vardır). Yeni alətlər son illər hakerlərin illik *BlackHat* konfransları çərçivəsində *BlackHat Arsenal* tədbirlərində nümayiş etdirilir. Burada yalnız bir neçə geniş yayılmış aləti göstərmək istərdik: eksployt platforması *Metasploit* (qrafiki interfeys üçün açıq kodlu *Armitage*); parolların sındırılması (*HashCat*; *Cain&Abel*); sniffer (*WireShark*); simsiz şəbəkələrə hücum (*Wifite*); sosial mühəndislik aləti (*SET*); veb proqramlarda boşluq skaneri (*OWASP ZAP – Zed Attack Proxy Project*); şəbəkə skaneri (*NMap*); bot şəbəkə aləti *Black Energy* 2 (2008-ci ildə Gürcüstana qarşı kiberhücumlarda istifadə edilib, 2-ci versiyada bir çox funksiya – spam göndərilməsi, məlumatların ələ keçirilməsi, proksi-server əlavə edilib).

Qabaqcıl kibersilahlar onların aşkarlanmasını və aradan qaldırılmasını əhəmiyyətli dərəcədə çətinləşdirən aşağıdakı bir sıra xüsusiyyətləri ilə adi viruslardan və troyanlardan fərqlənirlər:

- zərərli proqramların formasını öz-özünə dəyişməsi;
- elektron sxemləri məhv etmək imkanları;
- zərərli proqramların öz-özünü şifrləməsi (deşifrləməsi);
- simsiz şəbəkələri kənardan pozmaq imkanları;
- geniş yayılmış kommersiya proqram təminatının açıqlanmamış boşluqlarından istifadə edilməsi.

Qabaqcıl kibersilahlardan kritik infrastruktur obyektlərinin və kritik texnoloji proseslərin idarəetmə sistemlərinə − *SCADA* (*Supervisory Control and Data Acquisition* dispetçer nəzarəti və verilənlərin toplanması) sistemlərinə kiberhücum və kibercasusluq üçün nəzərdə tutulmuş alətləri diqqətə almaq lazımdır. Cəmiyyət elektrik, su təchizatı, nəqliyyat, rabitə, bank və s. infrastrukturundan yüksək dərəcədə asılıdır. Bu kritik infrastruktur obyektləri *SCADA* sistemləri vasitəsilə əlyetərlidirlər və onlara istənilən yerdən qoşulmaq mümkündür. Nəticədə, hətta İnternetdən dolayısı ilə istifadə edənlər də təsirə məruz qalırlar.

Kritik texnoloji prosesləri hədəfə alan ən məşhur zərərli proqram 2010-cu ildə Belorus antivirus şirkəti *BlokAda* tərəfindən aşkarlanmış *Stuxnet* virusudur. *Stuxnet* virusu ilə 2010-cu ildə İranın nüvə mərkəzləri hədəfə alınmışdı. Aparılan analizlər nəticəsində virusun 2009-cu ildə yazıldığı, 4 ədəd 0-gün boşluğundan istifadə edildiyi və virusun fləş disklərlə yayıldığı aşkarlanmışdı [14].

Stuxnet aşkarlandıqdan sonra nüvə enerjisi mərkəzlərinə və ya kritik infrastruktur xidmətləri göstərən digər sənaye idarəetmə sistemlərinə yönəlik hücumlar edən, yaxud məxfi məlumatları oğurlayan mükəmməl kibercasusluq alətləri (*Advanced Persistent Threat, APT*) kimi bilinən digər viruslar da (*Duqu, Flame, Gauss*) aşkarlandı. *Duqu* virusu e-poçtla yayılırdı və *Microsoft Word* proqramındakı bir təhlükəsizlik boşluğundan istifadə edərək İrandakı nüvə mərkəzlərinə aid məlumatları toplayırdı. *Duqunun* yaradıcıları ya *Stuxnet* virusunun yazarları ilə eynidirlər, ya da *Stuxnet* virusunun ilkin kodunu araşdırmaq imkanları olmuşdur.

Flame virusu *Stuxnet* ilə müqayisədə dəfələrlə mürəkkəb quruluşa malikdir, onun 2010-cu ilin avqustundan fəal işə başladığı təxmin edilir. *Flame* sızdığı kompüterdə gizlənmək üçün özünü 5 müxtəlif şifrləmə alqoritmi ilə şifrləyir. 20 müxtəlif moduldan ibarət olan *Flame* 20 MB həcmindədir. İran *CERT*-inin (*Maher*) verdiyi məlumata görə, 43 antivirus onu aşkarlaya bilməmişdi. Bu virus insan tərəfindən analiz yolu ilə təsbit edilmişdi. *Kaspersky Lab* ekspertlərinə görə, virusun şifrlərinin çözülməsi illərlə vaxt tələb edir [15].

Gauss müəyyən ölkələrdən böyük həcmdə bank və maliyyə məlumatları oğurlamağa yönəlib. Təhlükəsizlik ekspertləri virusun layihələndirilməsinə və proqramlaşdırılmasına 5 il vaxt sərf edildiyini, yüksək ixtisaslı bir komanda tərəfindən hazırlandığını və arxasında mütləq bir dövlətin durduğunu irəli sürürlər.

Stuxnet virusunun və onun ardıcıllarının (*Flame, Gauss, Duqu*) analizi göstərir ki, bu zərərli proqramları hansısa haker qrupu deyil, dövlət dəstəkli təşkilat(lar) yaradıb. Belə virusların hazırlanmasına on milyonlarla dollar vəsait sərf edildiyi güman edilir. Bundan başqa, bu viruslar o qədər mürəkkəbdirlər ki, onları mütəxəssislərin böyük qrupu bir neçə il (məsələn, *Gauss* – 5 il) ərzində hazırlaya bilərdi [15].

"*Elderwood* layihəsi" kibersilahların sənaye üsulu ilə hazırlanmasını və eyni zamanda, kiberfəzada kəşfiyyat və kiberhücumların avtomatlaşdırılmasını təsdiq edir [16].

Symantec firmasının "*Elderwood* layihəsi" ilə əlaqəli hazırladığı hesabatda istifadə edilən 0-gün boşluqlarının sayının nisbətən çox olması *Elderwood* platformasının fərqləndirici xüsusiyyəti kimi göstərilir [16]. Bir çox hücumda eksployt kodunun haradan götürüləcəyini müəyyən edən dəyişənə "*Elderwood*" adı verilir. Bu səbəbdən platforma və layihəyə "*Elderwood*" adı verilmişdir.

Bundan başqa, kiberfəzanın dinamik şəbəkə infrastrukturunda real vaxt rejimində irimiqyaslı hücum əməliyyatlarının işlənməsi, planlaşdırılması və həyata keçirilməsinə imkan verən yeni texnologiyaların yaradılması sahəsində genişmiqyaslı elmi-praktiki işlər də aparılır (X Planı). ABŞ Müdafiə Nazirliyi *DARPA* tərəfindən işlənib hazırlanan və son illər ərzində həyata keçirilən X Planı sırf texniki məqsədlərlə yanaşı, kibermüharibələrin təbiətinin, strategiyaların və fundamental taktikaların işlənməsini də nəzərdə tutur [17]. Kibermüharibə meydanında üstünlüyü təmin etmək üçün aşağıdakı dörd əsas istiqamətə xüsusi fikir verilir:

1) kiberəməliyyatların planlaşdırılması üçün avtomatik analiz metodlarının işlənməsi;
2) kiberəməliyyatların avtomatik idarə edilməsi texnologiyalarının yaradılması;

3) düşmən mühitdə konkret əməliyyatların aparılması üçün əməliyyat sistemlərinin və spesifik platformaların inkişaf etdirilməsi;
4) kiberdöyüş meydanının iri miqyasda interaktiv vizuallaşdırılması.

Ölkələrin kiberqoşun potensialı

Şimali Koreyanın kiberqoşun potensialının analizinə aid bir neçə açıq mənbə məlumdur [18]. Bu ölkənin kiberqoşunu bir neçə kiberbölmədə (*Office 91, Unit 121, Lab 110, Unit 35, Unit 204*) təşkil olunmuş 3000 elit hakerdən ibarətdir.

Office 91-in Şimali Koreya hakinq əməliyyatlarının baş qərargahı olması güman edilir, hakerlərin əksəriyyəti *Unit 121*-ə məxsusdur, hakinq və şəbəkələrə sızma əməliyyatlarının çoxu *Unit 121* tərəfindən həyata keçirilir. Onun əməliyyatları Şimali Koreyadan kənarda həyata keçirilir və xaricdə, xüsusən də Şimali Koreya sərhədinə yaxın Çin şəhərlərində yardımçı ofisləri var.

Lab 110 adlanan bölmə də oxşar əməliyyatları yerinə yetirir. Hakimiyyətin digər qollarının tabeliyində də bir neçə kiberbölmə vardır.

Unit 35 kiberagentlərin təlimi üçün cavabdehdir və anlaşıldığına görə ölkədaxili kibertəhqiqatları və əməliyyatları idarə edir.

Unit 204 onlayn casusluq və psixoloji müharibədə iştirak edir.

Office 225 Cənubi Koreyada işləyəcək agentlərin təlimini həyata keçirir, bəzən onların işində kiber komponent də ola bilər.

Şimali Koreya 2009-cu ildə Cənubi Koreyaya 6 böyük kiberhücum təşkil etmişdi ki, vurulan zərər 780 milyon dollar həcmində qiymətləndirilirdi. Buna cavab olaraq, 2010-cu ildə Cənubi Koreyada kibermüdafiə komandanlığı yaradılıb. Cənubi Koreya öz kiber-müdafiə bölməsinin sayını iki dəfə artıraraq 2030-cu ildə 1000 nəfərə çatdırmağı planlaşdırır.

Çin hələ 1999-cu ildən şəbəkə müharibələrinə hazırlaşmağa başlamışdı. Çinin Amerika şirkətlərinin istehsal texnologiyalarının oğurlanmasına yönəlmiş haker fəaliyyəti iki ölkə arasında çoxdan mübahisə mənbəyidir. Amerika ekspertləri Çinin iqtisadi casusluğu nəticəsində vurulan ziyanın 300 milyard dollardan artıq olduğunu bildirirlər. Bəzi KİV baş verənləri "soyuq kibermüharibə adlandırır". Çin Amerika şirkətlərinə qarşı kibercasusluq və həmin ölkənin kritik infrastrukturlarına kiberhücum ittihamlarını israrla rədd edir. Ekspertlərə görə, hazırda Çin kiberordusu 6 minə yaxın hakerdən ibarətdir [19].

Çin Xalq Azadlıq Ordusunun elmi-tədqiqat institutu tərəfindən 2005-ci ildə nəşr edilmiş "Hərbi strategiya elmi" (*The Science of Military Startegy*) ensiklopediyasında ilk dəfə kiberqoşunlar Çin Xalq Respublikasında qoşun növləri arasında göstərilir [20]. Ensiklopediyada Çin kiberqoşunları 3 sinfə ayrılır. "Hərbiləşdirilmiş xüsusi kompüter qoşunları"nın vəzifəsi kiberhücumlardan müdafiə və kiberhücumların həyata keçirilməsidir. İkinci sinfə "şəbəkə döyüş əməliyyatları" yerinə yetirmək hüququ verilən mülki mütəxəssislər daxildir (20 minə yaxın "vətənpərvər-haker"). Nəhayət, üçüncü sinfə hökumətə aid olunmayan "kənar elementlər" daxildir ki, onları şəbəkələrdə ziyanlı hərəkətlərin yerinə yetirilməsi üçün səfərbər etmək olar (2 milyona yaxın agent).

İsrail həyati əhəmiyyətli infrastrukturları kiberhücumlardan qorumaq məqsədi ilə rəqəmsal "Dəmir Qübbə" yaratmaq planını həyata keçirir, bura əhəmiyyətli resurslar investisiya edir. Milli proqram çərçivəsində 16-18 yaşlı istedadlı şagirdlər üçillik kurslarda kiberhücumların qarşısını almaq sənətinə yiyələnirlər.

İspaniya kibermüdafiə komandanlığının tərkibində tam funksional vəziyyətdə 70 mütəxəssisin olması nəzərdə tutulur (Madrid yaxınlığındakı Retamares hərbi bazası). Kiberkomandanlıq silahlı qüvvələrdə informasiyanın tamlığının və konfidensiallığının təmin edilməsinə cavabdehdir və informasiya təhlükəsizliyi insidentlərinin emalı mərkəzlərinin fəaliyyətini koordinasiya etməyə və yönləndirməyə məsuldur.

ABŞ xüsusi xidmətləri və hərbi strukturları arasında kibertəhlükəsizlik sahəsində səlahiyyətlər uğrunda ciddi rəqabət mövcuddur. Hərbçilərin kiberfəzada bütün fəaliyyətini təmin

etməyi öz üzərinə götürən birləşmiş kiberkomandanlığın yaradılması vəzifəsi hələ 2002-ci ildə Strateji komandanlığa tapşırılmışdı, lakin şəbəkədə hərbi əməliyyatların aparılması faktiki olaraq Hərbi Hava Qüvvələrinin (HHQ) üzərində idi və 2007-ci ildə HHQ bazasında (Barksdeyl, Luiziana) ilk kiberkomandanlıq yaradılmışdı.

HHQ-nin belə aşkar dominantlığı digər qoşun növlərinin strukturlarında qəbul edilmirdi. Uzun diskussiyalardan sonra əsas qoşun növlərinin funksiyalarını inteqrasiya edən və qarşılıqlı əlaqələrini təmin edən inteqrativ strukturun yaradılması qərara alındı və 2009-cu ilin iyununda ABŞ Strateji Komandanlığının tabeliyində bu ölkənin kiberkomandanlığı (*US CyberCom*) yaradıldı. Onun əsas vəzifəsi ABŞ və müttəfiqlərinin kiberfəzada fəaliyyətinin sərbəstliyini təmin edən və düşmən ölkələrin sərbəst fəaliyyətini məhdudlaşdıran əməliyyatların həyata keçirilməsidir. ABŞ kiberkomandanlığının struktur-təşkilati modeli digər ölkələr üçün nümunə ola bilər.

US CyberCom 2013-cü ildə kiberqoşunların sayını 5 dəfə artıraraq 900-dən 4900-ə çatdırmağı planlaşdırırdı. ABŞ-da kiberqoşunların inkişafında növbəti addım kibermüharibə kəşfiyyat mərkəzinin yaradılmasıdır (*Cyber Warfare Intelligence Center*).

Rusiyada ordunun informasiya təhlükəsizliyinə cavabdeh kiberkomandanlığın ABŞ və NATO modelinə uyğun yaradılması 2014-cü ilə planlaşdırılmışdı (bəzi mənbələr bu müddətin 2016-cı ilə qədər uzadılmasını göstərir). Kiberqoşunların riyaziyyatçılar, proqramçılar, mühəndislər, kriptoqraflar, rabitəçilər, radio-elektron mübarizə mütəxəssisləri, tərcüməçilər və digər yüksək ixtisaslı mütəxəssislərlə komplektləşdirilməsi nəzərdə tutulur. Eyni zamanda, Amerika təşkilatı *DARPA*-ya oxşar perspektiv müdafiə tədqiqatları fondunun yaradılması üzrə də işlərin aparılması açıq mətbuatdan məlumdur.

2008-ci ildə Tallində NATO Kibermüdafiə Mərkəzi quruldu və ona beynəlxalq hərbi təşkilat statusu verildi. Qeyd edək ki, 2009-cu ildə NATO "kibertəhlükəsizlik" terminindən "kibermüdafiə" terminina keçdi və kiberlayihələrə ayrılan büdcəni 40 dəfə artırdı. NATO-nun 2010-cu ilin noyabrında qəbul edilmiş yeni strateji konsepsiyasında kibermüdafiə prioritet fəaliyyət istiqamətlərindən biri kimi müəyyən edildi. Kommunikasiya sistemlərinin və infrastrukturun müdafiəsi üçün kiberhücumlara çevik reaksiya qüvvələrinin yaradılması, kiberhücumlara məruz qalan ölkələrə zəruri yardım və dəstəyin göstərilməsi nəzərdə tutulurdu.

2013-cü il iyunun əvvəlində NATO ölkələri müdafiə nazirlərinin görüşündə kiberqoşunların yaradılması haqqında qərar qəbul edildi. Ümumi kibermüdafiə sisteminin həmin ilin payızına kimi işə salınması nəzərdə tutulurdu. Sonrakı mərhələdə kommunikasiya sistemlərinin və infrastrukturun müdafiəsi üçün zəruri resursların yaradılması planlaşdırılırdı.

Kibersilahların xüsusiyyətləri

Adi silahlarla kibersilahlar arasında (yaradılması, yayılması, sınaqdan çıxarılması, istifadəsi, köhnəlməsi, xərclər və s. baxımından) əhəmiyyətli fərqlər vardır [21].

Kibersilah hədəf sistemindəki boşluqlar haqqında biliklər əsasında yaradılan proqram kodu və ya istifadəçi ilə boşluğun olduğu sistem arasındakı qarşılıqlı təsirdir. Kiberhücumlar yalnız mümkün boşluqları gizli saxladıqda mümkündür. Əgər hədəf sistemində kibersilahın istifadə etdiyi boşluq aşkarlansa və aradan qaldırılsa, onda kibersilah yararsız olur.

Kibersilah arsenalını yeni silahlarla genişləndirmək üçün yeni boşluqlar tapmaq tələb edilir. Bu baxımdan, kiberqoşunların tərkibində ən qiymətli kadrlar proqram təminatında boşluqları aşkarlamağı bacaran mütəxəssislərdir.

Boşluqlar, onlar haqqında biliklər və onları istismar etmək üzrə bacarıqlar kibermünaqişənin istənilən formasında xüsusi əhəmiyyət daşıyır. Aydındır ki, istismar edilən boşluqlar olmasaydı, kiberhücumlar *(D)DoS* və hədəf sisteminə girmək üçün sosial mühəndislik vasitəsilə istifadəçilərin manipulyasiyası ilə məhdudlaşardı. *(D)DOS* hücumlar hədəf sistemindəki boşluqlara əsaslanmır, kommunikasiya kanalının buraxılış zolağını, mərkəzi prosessoru və ya digər məhdud resursu tükətməklə sistemin əlyetərliyini məhdudlaşdırır.

Kibersilahların yaradılması üçün həm məlum (açıqlanmış) boşluqlar, həm də hələlik açıqlanmamış boşluqlar (sıfır-gün boşluqları) istifadə edilir. İl ərzində aşkarlanan sıfır-gün boşluqlarının orta hesabla sayı çox deyil, *Symantec*-in hesabatına görə, 2011-ci ildə 8 sıfır-gün boşluğu aşkarlanmışdı [22]. Kibersilahların istehsalı üçün sıfır-gün boşluqları xüsusi əhəmiyyət daşıyır, lakin məlum boşluqlar da geniş istifadə edilir. Məsələ ondadır ki, bəzi boşluqlar açıqlandıqdan on illər sonra da aradan qaldırılmamış qalır [21].

Aşkarlanmış boşluqların açıqlanması üçün müxtəlif strategiyalar mövcuddur (məsələn, RFPolicy) [11]. Qeyd edək ki, boşluqların "qara bazarı" da mövcuddur, burada sıfır-gün boşluqları əldə etmək mümkündür. Adətən, boşluq məlum olduqdan sonra, istehsalçı boşluğu aradan qaldırmaq üçün qısa müddətdə proqram təminatına düzəlişlər ("yamaqlar") hazırlayır və istifadəçilər üçün əlyetərli edir. Bu düzəlişlər istifadəçilər tərəfindən izlənilməli və vaxtında quraşdırılmalıdır.

İnformasiya texnologiyalarının dinamik mahiyyətinə görə boşluqlar çoxluğu zamana görə dəyişir, hər gün yeni boşluqlar açıqlanır. Məlum boşluqlar haqqında bir sıra məlumat bazaları, göndəriş siyahıları, ödənişli və ya ödənişsiz məlumat xidmətləri mövcuddur. Məlum boşluqlar üzrə mötəbər mənbə ABŞ Milli Standartlar və Texnologiyalar İnstitutu tərəfindən yaradılmış Vahid Boşluqlar Bazası hesab olunur [11].

Boşluqlar ciddiliyinə görə fərqlənir. Bəzi boşluqlar düşmənə hədəf sisteminə kiberhücumlar təşkil etməyə imkan verir, bəzilərinin isə hücum edənə heç bir faydası yoxdur. *CVSS* sistemi boşluqların unikal xüsusiyyətləri, zamana görə davranışı və mühit xarakteristikaları əsasında boşluqların ciddiliyini qiymətləndirməyə imkan verən metod təqdim edir [11].

Kibersilahların istehsal xərcləri, əsasən, cəlb edilən insan resursları ilə əlaqəlidir. Elmi tədqiqatlara və layihə-konstruktor işlərinə ilkin investisiyalar zəruridir, lakin təkbaşına hakerlərin və kiçik qrupların (məsələn, *Anonymous*, *Lulzsec*) uğurları göstərir ki, məhdud resurslarla da çox şeyə nail olmaq olar. Müasir adi silahların yaradılması ilə müqayisədə kibersilahların yaradılması dövlətlər üçün daha az xərc tələb edir. Kibersilahlar insan biliyi və nisbətən ucuz kompüter avadanlığı əsasında yaradılır. Proqram mühəndisliyi, eksployt mühəndisliyi və nüfuzetmə testləri sahəsində biliklər (və bacarıqlar) kiberhücumların əsasıdır. Düzgün seçilmiş mütəxəssislərin cəlb edilməsi, onların biliyinin artırılması kibersilah arsenalını saxlamaq və genişləndirmək üçün zəruri sərmayədir. Hədəfin boşluqlarını və onlardan necə istifadə etməyi bilmək hücum edən üçün olduqca əhəmiyyətlidir. Digər tərəfdən, bu bilik hücum hədəfində effektiv müdafiəni qurmaq üçün də çox vacibdir.

Bu kibersilahların birinci paradoksuna gətirir [21]: kibersilahlar zaman keçdikcə tənəzzül edirlər. Əgər kibersilah müəyyən boşluğu istismar edirsə, onun effektivliyi hədəf sistemində bu boşluq mövcud olana kimi davam edir.

Kibersilahların ikinci paradoksu [21] – kibersilahların istifadəsi hədəf sisteminin müdafiəsini gücləndirməyə gətirib çıxara bilər. Kibersilah tətbiq edildikdən sonra, hədəf bu hücumu aşkarlaya və onun necə yerinə yetirildiyini analiz edə bilər. İlk hücum uğurlu ola bilər, lakin bundan sonra müvafiq müdafiənin qurulacağı ehtimalı da xeyli yüksəkdir və bu həmin kibersilahı yararsız edir.

Bu kibersilahların test edilməsinə də müəyyən məhdudiyyətlər qoyur. Müəyyən kibersilah test edildikdən sonra bu təhlükədən xəbər tutan hədəflərin həmin hücumdan müdafiə olunmaq yolunu tapacaqları ehtimalı kifayət qədər yüksəkdir.

Adi fayllar kimi bu kibersilahları da xərc çəkmədən nüsxələmək olar, buna görə kibersilahların sayı qeyri-adi dərəcədə çoxdur. Kibersilahların saxlanması və nəqli də adi silahlardan çox asandır. Kibersilahın nüsxəsini və ya bütün kibersilah arsenalını İnternetin müxtəlif yerlərində gizlətməklə ölkə sərhədindən kənarda saxlamaq olar.

Kibersilah fiziki təbiətə malik deyil, onlar bilik və verilənlərdən ibarətdir. Kibersilahı istifadə etmək üçün hücum edən hədəfə verilənləri çatdırmalıdır. Bunu, məsələn, skript və ya

proqram yazaraq onu informasiya sistemində çoxaltmaqla avtomatlaşdırmaq və davamlı etmək olar.

Kiberqoşunlar üçün insan resurslarının hazırlanması

"ABŞ-a hücum etmək üçün kiberordunu necə yaratmalı" [23] məqaləsində kiberqoşun üçün aşağıdakı mütəxəssislər heyəti təklif edilir (mötərizədə nəfər sayı göstərilib) – boşluqlar üzrə analitiklər (10), eksployt proqramçıları (70), məsafədəki heyət (20), bot toplayıcıları (60), bot xidmətçiləri (220), operatorlar (60), proqramçılar (40), testçilər (15), texniki məsləhətçilər (20), sistem administratorları (10), menecerlər (57).

Kiberqoşunların formalaşdırılmasında ən böyük problemlərdən biri kadr təminatıdır. Peşəkarlar çatışmır və informasiya təhlükəsizliyi üzrə mütəxəssisləri dövlət təşkilatlarında işləməyə cəlb etmək üçün dövlət əlverişli şərtlər təklif etməkdə özəl strukturlarla rəqabət apara bilmir. Bu problem ölkələrin əksəriyyəti üçün xarakterikdir.

Kiberqoşunlar üçün insan kapitalının inkişafında elm, texnologiya, mühəndislik və riyaziyyat (*STEM – science, technology, engineering, and mathematics*) sahəsində təhsil alan tələbələrin sayı və keyfiyyəti mühüm göstəricidir. Bu profildən olan insan kapitalından kiberqoşunların formalaşdırılmasında istifadə etmək daha məqsədəuyğundur.

ABŞ Hərbi-Dəniz Akademiyasında (*Annapolis*) kiberəməliyyatlar üzrə mütəxəssislər hazırlanır (ilk buraxılış 2016-cı ilə planlaşdırılır). Akademiya rəhbərliyinin bu kursun tədris proqramlarının hazırlanmasına təxminən 5 il vaxt sərf etdiyi söylənilir. Təhsil müddətində gələcək mütəxəssislər haker texnologiyaları ilə yanaşı, kibersiyasət və iqtisadiyyatı əhatə edən məcburi kursları da öyrənəcəklər. Tələbələrin mülki informasiya texnologiyaları şirkətlərində, həm də Milli Təhlükəsizlik Agentliyi və Federal Təhqiqat Bürosu kimi dövlət strukturlarında təcrübə keçmək imkanı olacaq.

İnformasiya təhlükəsizliyi üzrə biliklərin sertifikatlaşdırılması sistemləri. İnformasiya təhlükəsizliyi sahəsində kadrların hazırlanmasında ali məktəblərlə yanaşı, bir sıra şirkətlərin (*SANS Institute, Microsoft, Cisco* və s.) və beynəlxalq konsorsiumların (*ISACA, (ICS)2, EC-Council* və s.) mütəxəssislərin biliklərinin sertifikatlaşdırılması sistemləri də mühüm rol oynayır. İnformasiya təhlükəsizliyi üzrə biliklərin sertifikatlaşdırılması sistemləri haqqında ətraflı məlumatı [11]-də almaq olar, burada yalnız etik haker sertifikatı (*CEH, Certified Ethical Hacker*) haqqında məlumat verilir.

E-kommersiya üzrə Şuranın (*EC-Council*) *CEHv8* imtahanı informasiya təhlükəsizliyi mütəxəssislərinin biliklərinin sertifikatlaşdırılması sahəsində önəmli sistemlərdən biridir və ABŞ Müdafiə Nazirliyi tərəfindən bəyənilmişdir. Bu sertifikat şəbəkə təhlükəsizliyi sahəsində müvafiq səviyyədə biliklərin olmasını təsdiq edir.

CEH sertifikatlı etik haker şəbəkə təhlükəsizliyi sahəsində ixtisaslaşmış mütəxəssisdir, hakerlərin istifadə etdiyi bilik və alətlərdən istifadə edir, hədəf sistemlərində zəif yerləri və boşluqları necə axtarmağı bacarır. *CEHv8* sertifikat imtahanı şəbəkə protokollarının, əməliyyat sistemlərinin, tətbiqi proqramların boşluqları, troyanlar, viruslar, rutkitlər, informasiyanın toplanması, şəbəkənin daranması və resursların inventarlaşdırılması, veb-serverlərin, simsiz şəbəkələrin sındırılması, informasiya təhlükəsizliyi vasitələrinin aldadılması, nüfuzetmə testləri, *DoS* hücumların, *SQL*-inyeksiya hücumlarının həyata keçirilməsi, seansların ələ keçirilməsi və s. kimi sahələri əhatə edir.

İnformasiya təhlükəsizliyi üzrə yarışlar. İnformasiya təhlükəsizliyi üzrə mütəxəssislərin real şəraitə yaxın şərtlərdə təlimi və təcrübə qazanması imkanlarından biri informasiya təhlükəsizliyi üzrə yarışlarda iştirak etməkdir. Hazırda informasiya təhlükəsizliyi üzrə müxtəlif məzmunlu, formalı və miqyaslı yarışlar keçirilir:

- veb-saytların təhlükəsizliyi (Hack This Site);
- sistem administratorları arasında VSFI sistemi üzrə yarışlar;
- kibertəhlükəsizlik yarışları (US Cyber Challenge);

- kibermüharibə oyunları (Over The Wire, DC3, NetWars);
- CTF (Capture The Flag – "Bayrağı ələ keçir") və s.

Bu yarışlardan ən populyarı *CTF* tipli komanda yarışlarıdır. Bir qayda olaraq, yarışlarda maşın kodunun analizi (*reverse engineering*), şəbəkələrin idarə edilməsi, şəbəkələrin və protokolların analizi, proqramlaşdırma, kriptoanaliz bacarıqları tələb olunur.

CTF tipli yarış ilk dəfə *DEFCON* haker konfransında keçirilib (1996-cı il, 4-cü *DEFCON*). Ali məktəblər arasında beynəlxalq distant *UCSB iCTF* yarışları ilk dəfə 2004-cü ildə Santa-Barbara şəhərində yerləşən Kaliforniya tərəfindən keçirilib. Rusiyada *CTF* yarışları 2008-ci ildə Ural Dövlət Universiteti, *HackerDom* komandası tərəfindən təşkil edilib. 2009-cu ildən tələbələr arasında beynəlxalq distant *RuCTF* yarışları keçirilir.

Hazırda bir çox universitetlər *CTF* yarışları keçirir (məs., *rwthCTF, CSAW CTF, HUST CTF, MIT/LL CTF, RuCTF*), hətta şirkətlər və bəzi təşkilatlar da *CTF* yarışları təşkil edirlər (məs., *Mozilla CTF, Phdays CTF, OWASP Global CTF,CODEGATE*). Orta məktəb şagirdləri arasında da *CTF* yarışları təşkil etmək təşəbbüsləri vardır (*Codegate Global Junior CTF*).

Kibertəhlükəsizlik üzrə təlimlər. Hazırda bir sıra ölkələrdə irimiqyaslı kibertəhlükəsizlik təlimləri keçirilir.

Cyber Storm 2006-cı ildən başlayaraq ABŞ-da iki ildə bir dəfə geniş miqyasda və real vaxtda keçirilən kibertəlimlərdir. Bu kibertəlim iştirakçılara özlərinin kiberhücumlara hazırlıq, müdafiə və cavablandırma imkanlarını qiymətləndirməyə şərait yaradır.

Oxşar təlimlər Avropada 2010-cu ildən keçirilir (*Cyber Europe 2010*). Bu təlimlərin gedişində Avropa Birliyi (AB) ölkələrində yerləşmiş e-idarəetmə infrastrukturunun kritik vacib elementlərinə qlobal *DDoS*-hücum imitasiya edilmişdi. Təlimlərin məqsədi AB dövlətlərində rəqəmsal infrastrukturun kritik obyektləri arasında rabitənin sıradan çıxmasına hazırlıq səviyyəsinin yoxlanması idi.

NATO-nun nümunəvi birgə kibermüdafiə mərkəzində (*NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE*, Tallində yerləşir) informasiya texnologiyaları sahəsində illik kibertəlimlər 2008-ci ildən keçirilir. 2013-cü ildə "Bağlı qalxanlar 2013" (*Locked Shields 2013*) adlı kibertəlimlər kiberhücumlara qarşı müdafiənin effektivliyi yoxlanılırdı və təlimdə Avropanın 9 ölkəsindən 250 mütəxəssis iştirak edirdi.

2011-ci ildə AB və ABŞ arasında *Cyber Atlantic 2011* adlı ilk kibertəhlükəsizlik təlimi keçirilib. Təlimlərdə AB-nin 20 ölkəsindən və ABŞ-dan yüzə yaxın mütəxəssis iştirak edirdi. İki ssenari istifadə edilirdi: 1) AB üzvü olan ölkələrdən məxfi informasiyanın əldə edilməsinə və nəşr olunmasına yönəlmiş APT-hücum (*Advanced Persistent Threat*, Genişləndirilmiş Davamlı Təhdid); 2) Avropa enerji təchizatı obyektlərində istifadə edilən sənaye *SCADA*-sistemlərinin kütləvi sıradan çıxması. Təlimlər çərçivəsində AB və ABŞ arasında qarşılıqlı əlaqə metodları da məşq edilirdi.

Kibertəhlükəsizlik sahəsində koordinasiya və beynəlxalq əməkdaşlıq məsələləri

Hazırda kibertəhlükəsizliyin təmin edilməsi ilə məşğul olan bölmələr digər dövlət strukturlarında da yaradılır və nəticədə, kibertəhlükəsizlik sahəsində məsuliyyət bir neçə struktur arasında paylaşılır. Bu strukturlar avtonom hərəkət edirlər və bəzən onların öz korporativ maraqlarından çıxış etməsi riski vardır. Buna görə də kibertəhlükəsizlik sahəsində koordinasiyanın bütün istiqamətlər üzrə təmin edilməsi olduqca vacibdir. Müxtəlif strukturların işini əlaqələndirən, qərar qəbul edilməsinin və dövlət siyasətinin həyata keçirilməsinin vahid mərkəzi kimi çıxış edən milli kibermüdafiə mərkəzini formalaşdırmaq təklif olunur.

Kibertəhlükəsizliyin təmin edilməsi sahəsində dövlət siyasətinin formalaşdırılması, kibertəhlükəsizlik sahəsində dövlət strukturlarının məsuliyyət sahələrini və səlahiyyətlərini müəyyən edən vahid normativ hüquqi sənədlərin qəbul edilməsi vacibdir.

Kiberfəzada dövlətlərin suverenliyinin təmin edilməsinin bəzi problemləri yalnız beynəlxalq və regional əməkdaşlığın inkişaf etdirilməsi, bu sahədə ölkələrin öz səylərini birləşdirməsi, etimadın və risklərin adekvat qiymətləndirilməsi şəraitində mümkündür.

Kiberfəzada tərksilah, kibertəhlükəsizlik strategiyalarının tam müdafiə xarakterli olması, sürətlə silahlanmanın dayandırılması, Rəqəmsal Cenevrə Konvensiyasının qəbul edilməsi ideyası da səsləndirilir – mülki əhali üçün elektrik, su, səhiyyə və s. kimi həyati əhəmiyyət daşıyan infrastruktura hücum edilməməlidir. Bu konvensiyanın pozulmasına müharibə cinayəti kimi baxılmalıdır.

Nəticə

Sürətlə dəyişən kiberfəzada ölkənin milli maraqlarını təmin etmək üçün silahlı qüvvələrin strukturunda kibertəhdidlərlə mübarizə aparan yeni bölmələrin yaradılması zəruridir. Bu həm silahlı qüvvələrin, həm də bütün ölkənin informasiya təhlükəsizliyinin təmin edilməsi üçün vacibdir. Kiberkomandanlığın formalaşdırılması, onun funksional vəzifələrinin müəyyən edilməsi, şəxsi heyətlə komplektləşdirilməsi əhəmiyyətli dərəcədə geniş idarəetmə səyləri, insan kapitalı və elmi-tədqiqatların ən yüksək səviyyədə təmin edilməsini tələb edir.

Ədəbiyyat

1. Əliquliyev R.M., İmamverdiyev Y. N. E-dövlətin informasiya təhlükəsizliyi: Aktual tədqiqat istiqamətləri // İnformasiya cəmiyyəti problemləri, 2010, №1, s. 3-13.
2. Clarke R.A., Knake R. Cyber War: The next threat to national security and what to do about it. Harper Collins 2010, 304 p.
3. Evron G. Battling botnets and online mobs. Estonia's defense efforts during the Internet War // Georgetown Journal of International Affairs, 2008, vol. 9, no. 1, pp. 121-126.
4. Hollis D. Cyberwar case study: Georgia 2008 // Small Wars Journal blog, 2010, http://www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf
5. Gumahad A. T. Cyber troops and net war: The profession of arms in the information age. BiblioScholar, 2012. 68 p.
6. Conti G., Surdu "Buck" J. Army, navy, air force, cyber: is it time for a cyberwarfare branch of the military? // Information Assurance Newsletter, 2009, vol. 12, no. 1, pp. 14-18.
7. Owens W.A., Dam K. W, Lin H. S. (eds.) Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities. National Academies Press, 2009, 390 p.
8. Geers K. Strategic cyber security. CCD COE Publication, Tallinn, Estonia, 2011, 168 p.
9. Ələkbərova İ.Y. İnformasiya müharibəsi texnologiyaları. Ekspress-informasiya. İnformasiya cəmiyyəti seriyası. Bakı: "İnformasiya texnologiyaları" nəşriyyatı, 2012, 108 s.
10. Libicki M. What is information warfare? // National Defense University, 1995, 110 p.
11. Əliquliyev R. M. , İmamverdiyev Y. N. İnformasiya təhlükəsizliyi insidentləri. Bakı: İnformasiya Texnologiyaları, 2012, 212 s.
12. Floridi L., Taddeo M. The ethics of information warfare. Springer. 2014, 145 p.
13. Hutchins E. M., Cloppert M. J., Amin R. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare and Security Research, 2011, pp. 78-104.
14. Langner R. Stuxnet: dissecting a cyberwarfare weapon // IEEE Security & Privacy, 2011, vol. 9, no. 3, pp. 49-51.
15. Gostev A. The Flame: questions and answers. 2012, http://www.securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51
16. O'Gorman G., McDonald G. Symantec security response report: The Elderwood Project. September, 2012, 137 p.
17. DARPA Information Innovation Office Programs: Plan X, http://www.darpa.mil/Our_Work/I2O/Programs/Plan_X.aspx

18. HP Security Briefing - Episode 16 “Profiling an enigma: The mystery of North Korea’s cyber threat landscape,” August 2014.
19. Mandiant. APT1: Exposing one of China’s cyber espionage units. February, 2013.
20. Peng G., Yao Y. (editors) The Science of Military Strategy. China Military Science Publishing House, 2005, 504 p.
21. Czosseck C., Podins K. A vulnerability-based model of cyber weapons and its implications for cyber conflict // International Journal of Cyber Warfare and Terrorism, 2012, vol. 2, no. 1, pp.14-26.
22. Dumitras T., Bilge L. Before we knew it: An empirical study of zero-day attacks in the real world / ACM Conference on Computer and Communications Security, 2012, pp. 833-844.
23. Miller C. Kim Jong-il and me: How to build a cyber army to attack the U.S., DefCon 18, 2010, http://www.defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf

УДК 004.9:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Кибервойска: функции, оружие и кадровый потенциал

Конфликты между странами переходят в киберпространство, и для осуществления операций в виртуальном пространстве в мирное и военное время начинают создаваться специальные виды войск - кибервойска. Для обеспечения информационной безопасности в некоторых странах существуют кибервойска или их планируется создать в ближайшие годы. В этой работе исследуются проблемы формирования кибервойск. Рассматриваются основные аспекты создания кибервойск, их задачи и функции, структурно-организационные модели киберкомандования, арсенал оружия кибервойск и человеческие ресурсы, анализируется опыт развитых стран в этой области. Обсуждаются также проблемы координации деятельности кибервойск и других государственных организаций, связанных с кибербезопасностью, и вопросы международного сотрудничества.

Ключевые слова: *информационная война, кибервойна, киберооборона, кибервойска, кибероружие, киберкомандование.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

Cybertroops: functions, arms and human resources

Conflicts between countries are transferred into cyberspace, and to carry out operations in the virtual space in peacetime and wartime start to be created special types of troops - cybertroops. To provide the information security of the country, in some countries, there are cybertroops or planned to create in the coming years. In this paper we study the problem of forming cybertroops. The main aspects of forming of cybertroops, tasks and functions of cybertroops, structural and organizational models of Cyber Command, arsenal of weapons and human resources of cybertroops are considered, and experience of developed countries in this field is analyzed. Problems of coordination of activities of cybertroops and other public organizations related to cyber security, and issues of international cooperation are also discussed.

Keywords: *information warfare; cyberwar; cyber defense; cybertroops; cyber weapons; Cyber Command.*