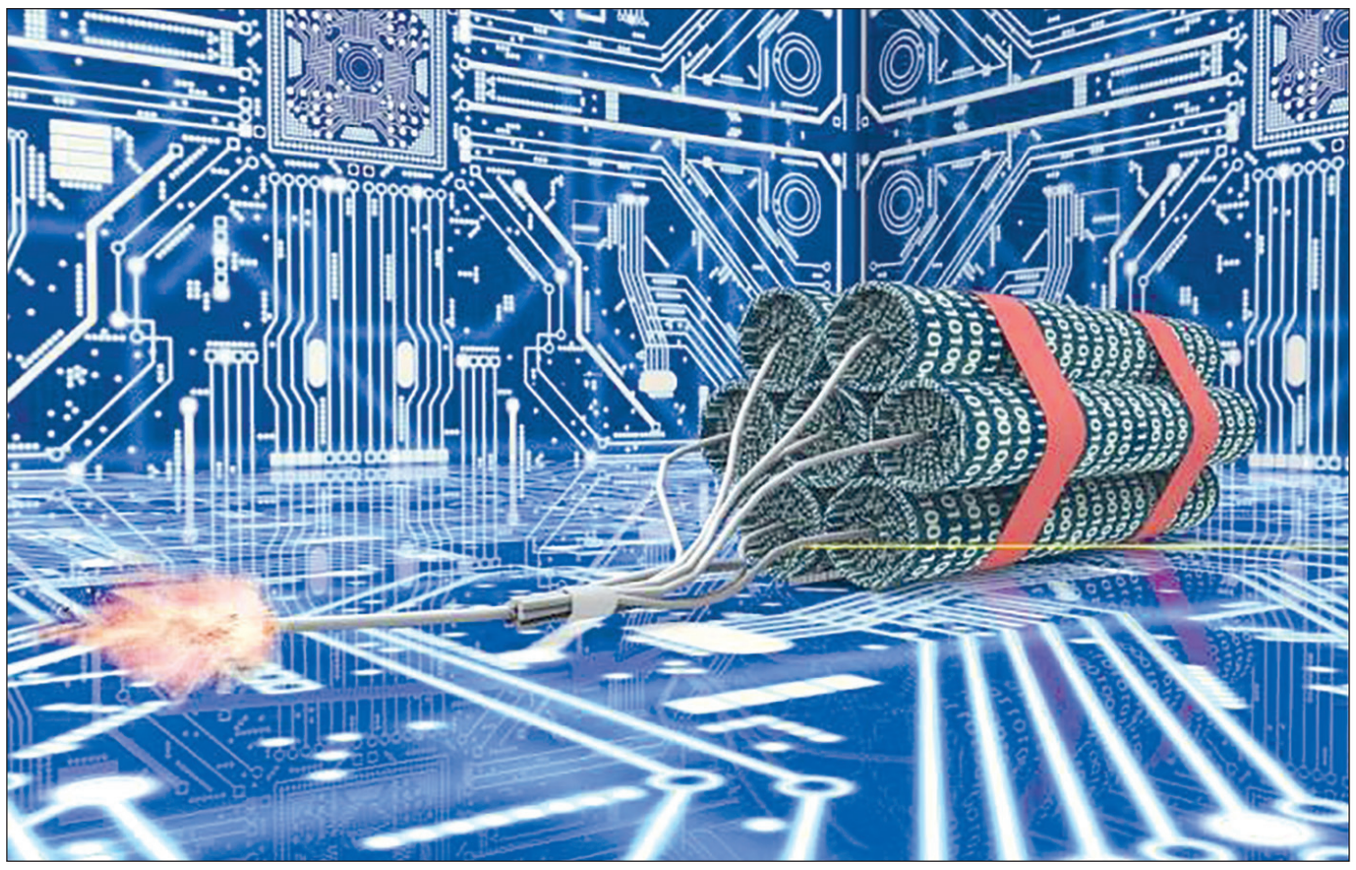
YENİ AZƏRBAYCAN
http://www.yeniazerbaycan.com
Azərbaycanın dövlət müstəqilliyi Azərbaycan xalqının milli sərvətidir

Kiberdünya - yeni güc, yeni təhdidlər



üzləşə biləcəyi deməkdir. "Sadə insana nə təhlükə var?" deməyin. Bu gün hər kəs nağdsız alış-verişlə, bank hesabları ilə hədəfdədir, barmağın ucundakı bir düyməyə basmaqla milyonluq transferlər etmək mümkünkən, planlı şəkildə kim bilir, nələr etmək olar.

Dünya başımız üzərindən asılmış peyklərin ayaqları altındadır. Təsəvvür edirsinizmi, bir gün hansısa bir cinayətkar qüvvə bu şəbəkələrə daxil olub onların işini pozsa, hansısa kompüter proqramları ilə işə salınan nüvə silahları nəzarətimizdən çıxsa, nələr olar? Çox uzaq keçmişə getmirəm, çox sadə bir nümunəni yada salmaq istəyirəm. 2018-ci ilin iyul ayında Mingəçevir İES-də yaranmış problem səbəbi ilə bütün ölkə bir neçə saat enerjisiz qalmaqla, nə böyüklükdə böhran yaşandı. Eyni problem kiberdünyada yaşansa, bu, bəlkə də milyonlarla insanın məhvinə gətirib çıxara bilər. Fəlakətin miqyasını təsəvvür etmək belə çətindir.

YENİ DÜNYA, YENİ SAVAŞ NÖVLƏRİ- KİBERMÜHARİBƏ

Bəşəriyyət hər nə qədər inkişaf etsə də, zəkası ilə kainatı fəth etməyə qalxsa da, ibtidai instinktindən, savaş istəyindən əl çəkməyib. Min illərdir insanların demək olar ki, ən böyük icadları məhz elə insan üzərində zəfər üçün kəşf edilib, min illərdir ən yeni kəşflər məhz insanları məhv etməyə, müharibə törətməyə hesablanıb. Leksikonumuza isə daha bir savaş termini daxil olub-Kibermüharibə.

Bu, siyasi məqsədlərə nail olmaq üçün ölkələr tərəfindən kiberhücumların istifadəsidir, kiberfəzada hərbi əməliyyatlardır. Bura həm hərbçilərin dövlətin silahlı qüvvələrinə qarşı döyüş hücumları (məsələn, düşmənin kritik vacib rabitə kanallarının sıradan çıxarılması), həm də mülki əhaliyə qarşı olan hücumlar daxildir. Kibercasusluq - hərbi, siyasi və iqtisadi üstünlüklər əldə etmək məqsədilə qiymətli konfidensial informasiyanın oğurlanmasıdır. Bir neçə il öncə Julian Asanjın sızdırdığı gizli materialların hansı siyasi qalmaqallara səbəb olduğunu yəqin unutmamışıq. Korporativ sistemlərə icazəsiz girişlər bir çox halda kibercasusluq məqsədləri daşıyır. Kibercasusluğun obyekti kimi çox zaman kommersiya sirri təşkil edən məlumatlar, intellektual mülkiyyət - istehsalat sirləri, marketinq planları, tədqiqatlar, məhsul nümunələri və hətta proqram təminatının ilkin kodları çıxış edir.

Kiber-təhdidlər, eyni zamanda, dünya iqtisadiyyatı üçün böyük təhlükə təşkil edir və vurulmuş ziyanın həcmi trilyonlarla ölçülür. 4-cü sənaye inqilabı dövrünü yaşayırıq, bu inqilab - istehsal proseslərində kiber-fiziki sistemlərin, süni intellektin, qlobal kommunikasiyaların geniş tətbiqi ilə xarakterizə olunur. Texnologiyaların sürətli inkişafı ilə kiber-təhdidlər də durmadan artır və genişlənir, onların qarşısını almaq üçün bütün ölkələr əhəmiyyətli xərclər çəkirlər. Beynəlxalq İqtisadi Forum 2014-cü ildən başlayaraq, kibertəhlükəsizliyi qlobal risklərin sırasına daxil edib. 2017-ci ildə keçirilmiş Forum yaxın on ildə qlobal inkişafı müəyyən edəcək ən yüksək 5 trend arasında cəmiyyət həyatının bütün sahələrində kiber-asılılığın artması tendensiyasını da göstərib. Forumun hesabatında kiberhücumlar və fərdi məlumatların oğurlanması, dələduzluq riskləri 10 ən yüksək risk arasında qeyd edilib.

Nəticədə qlobal kibertəhlükəsizlik sənayesi formalaşır və hazırda yüksək templə inkişaf edir. Bu sahənin özünəməxsus innovasiyaları, hərəkətverici qüvvələri, oyunçuları var. Forbes-in qiymətləndirmələrinə görə, qlobal kibertəhlükəsizlik bazarının həcmi 2015-ci ildə 75 milyard dollar, 2020- ci ildə 170 milyard dollar təşkil edib. Bazarın illik artımı 2015- 2020-ci illərdə 9,8% olub. Kibertəhlükəsizlik sahəsində sığorta ümumi sığorta bazarının ən sürətlə artan istiqamətlərindən biridir, əsasən ABŞ-da yayılıb. 2020-ci ildə qlobal kibertəhlükəsizlik sığorta bazarında illik satışların həcmi 7,5 milyard dollar olub.

DRON MÜHARİBƏLƏRİ

44 günlük haqq savaşımızda dünya sayəmizdə yeni dron müharibəsi ilə tanış oldu. Xaricdən alınan silahlara qoyulan şifrələr, süni beyinlər, satılan bütün silahların içərisində gizlədilmiş izləmə cihazları, xüsusi proqramlar - bu barədə dəfələrlə eşitmişik və bunlar şəhər əfsanələri deyil. Elə ona görə də, dünyanın ən güclü dövlətlərində belə fikir formalaşıb ki, sən silahı xaricdən alırsansa, istehsalçı qarşısında zəifsən, əliyalınsan.

Kibertəhlükəsizlik sənayesi inkişaf etdikcə məhsullarda süni intellekt inqilabı da paralel gedir. Kibertəhlükəsizlik sahəsinə Machine Learning və Big Data texnologiyalarının tətbiqi yeni nəsil kibertəhlükəsizlik alətlərinin meydana çıxmasına və bu da öz növbəsində analitika texnologiyalarına çəkilən xərclərin artmasına səbəb olacaq. Araşdırmalar zamanı məlum olub ki, bir çox zərərli proqram viruslarını hansısa haker qrupu deyil, dövlət dəstəkli təşkilatlar yaradır. Onların hazırlanmasına on milyonlarla dollar vəsait sərf edilir və ərsəyə gəlmələri bəzən illərlə zaman alır. Kibersilahların istehsal xərcləri əsasən cəlb edilən insan resursları ilə əlaqəlidir. Müasir adi silahların yaradılması ilə müqayisədə kibersilahların yaradılması dövlətlər üçün kiçik xərclərdir. Ən önəmlisi insan kapitalı, mütəxəssis yetişdirməkdir. Bax, bu sahə bizim zəif nöqtəmizdir. Kadr varsa da, sayları azdır.

Sadə insanlarınsa özlərinə təhlükə gördükləri kibertəhdid haker müdaxiləsidir. "Hakinq" termini ilə ifadə olunan bu əməl, hər hansı bir informasiya sisteminə hüquqa zidd olaraq, sahibindən xəbərsiz, razılığı olmadan daxil olmaqdır. Bu, bir kibercinayət hadisəsidir və bu əməl bir çox ölkələrdə olduğu kimi bizim ölkəmizdə də qadağandır, ümumi bir cinayət hadisəsi olmaqla bərabər, insan haqlarına ziddir, şəxsi həyata müdaxilə və başqa cinayətləri də özündə ehtiva edir.

Payızın əvvəlində İsrail əsilli hakerlər (İran belə iddia edirdi) İranın nüvə proqramı əsasında fəaliyyət göstərən nüvə santrallarının informasiya bazalarına kiberhücumlar təşkil edərək, təsisatın məxfi məlumatlar bazasını ələ keçirmişdilər. Bu məlumatı müxtəlif ölkələrin xəbər saytları paylaşdı. Yəqin bu faktdan sonra söz açdığımız mövzunun nə dərəcədə diqqətəlayiq olduğu aydınlaşır.

Kompüter şəbəkələrinin, elektron məlumatların cinayətlərin törədilməsi üçün istifadə edilməsi və bu növ cinayətlərin baş verməsinə dair sübutların bu şəbəkələrdə saxlanılması və ya şəbəkələr vasitəsilə ötürülməsi təhlükəsindən narahat olaraq dünya dövlətləri tərəfindən hələ 20 il öncə "Kibercinayətkarlıq haqqında" Konvensiya qəbul edilib. Bu sazişə Azərbaycan da qoşulub.

AZƏRBAYCAN PREZİDENTİNİN ÇOXLARINA QARANLIQ QALAN VACİB FƏRMANI

2021-ci il aprel ayının 17-də Azərbaycan Prezidenti İlham Əliyev "Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində tədbirlər haqqında" Fərman imzaladı. Bəziləri bunun nə demək olduğunun fərqinə belə varmadılar.

Kritik İnformasiya İnfrastrukturları (Kİİ) subyektlərinə - strateji vacib dövlət əhəmiyyətli sahələrə aid müəssisələr, təşkilatlar məsələn, səhiyyə, elm-təhsil, nəqliyyat, rabitə, energetika, bank sferası, neft-qaz kompleksi, atom enerjisi sahəsi, müdafiə sənayesi sahələri, kosmik-raket, dağ-mədən, metallurgiya və kimya sənayesi, o cümlədən, Kİİ şəbəkələrinin və ya sistemlərinin qarşılıqlı əlaqəsini təmin edən qurumlar aiddir. Yəni həyatımızı əhatə edən hər şey var. Bütün həyati sahələr üzrə qlobal miqyasda yaşanan böhranlı vəziyyətlərin ən sıxıntılı fazasına daxil olduğumuz indiki kritik dövrdə Prezidentin bu Fərmanının əhəmiyyəti hədsiz dərəcədə böyük idi və gələcəyə də hesablanıb.

İnformasiyaların mühafizə edilməsi və tətbiq olunması elminin tarixi son yüz illə məhdudlaşmır. Ta qədim zamanlardan başlayaraq, ölkələri idarə edənlər və ordu komandanları üçün mühüm hərbi, iqtisadi, siyasi və sosial yönümlü məlumatları həmişə məxfi saxlamaq zərurəti yaranıb. Vaxt keçdikcə, informasiya texnologiyaları və kriptoqrafiya perqamentləri gizli yazı ilə əvəz olundu, ancaq bəllidir ki, dövlət adamlarının hədəfləri dəyişməz olaraq qalır: dövlət və sənaye əhəmiyyətli sirləri qoruyub saxlamaq, informasiyaları kəşfiyyat-diversant agentlərinin qanun pozuntularından mühafizə etmək, təxribatçı kiberbasqınçılar tərəfindən təşkil olunan kiber hücumlar nəticəsində qəzaların və fəlakətlərin qarşısını almaq hər zaman mövcud olub. İndi demək olar ki, hansısa vacib məlumatlar kağız şəklində saxlanmır, ya da bu, çox az rast gəlinən hadisədir və informasiyalar analoji (rəqəmsal olmayan) sistemlərə tətbiq olunmur, elə bu səbəbdən onların qorunma metodları da rəqəmsal olmalıdır. Divin canı şüşədə olan kimi, indi dünyanın canı da rəqəmsal texnologiyalardadır.

Dövləti ciddi sıxıntılarla qarşıqarşıya qoya biləcək kiber təhdidlər və bənzəri hallara qarşı tədbirli, hazırlıqlı olmaq üçün Azərbaycanın dövlət başçısı belə bir fərmana imza atıb. Azərbaycanın qlobal dünyanın ayrılmaz tərkib hissəsi kimi, onun informasiya məkanı, xüsusilə də məxfi, gizli saxlanan informasiya bloku xarici və daxili kiber-hücumlardan sığortalanmayıb. Fərman var, qanunlar var. Qalır bu sahənin inkişafına, kadr potensialının artırılmasına dayanmadan səy göstərmək. Çünki hər keçən gün yüksək texnologiyalar yenilənir, inkişaf edir. Süni intellektlə insan arasında yarış gedir. Ümid edək ki, bu yarış növbəti onillikdə insanla süni intellektin savaşı səviyyəsinə çıxmaz. Biz hazır olmalıyıq.

İlhamə Rəsulova