Hibrid müharibə: rəqəmsal platformadan seçki qutusuna

Yerli və xarici kəşfiyyat dairələrinin son hesabatları həyəcan təbili çalır: Ermənistanda cari il iyunun 7-də keçiriləcək parlament seçkiləri yaxınlaşdıqca, ölkəyə qarşı aparılan gizli savaş daha sistemli, genişmiqyaslı və təhlükəli xarakter almağa başlayıb.

(ardı 6-cı səhifədə)

(əvvəli 1-ci səhifədə)

Bu mürəkkəb "müharibənin" əsas iştirakçılarını analiz edərkən həm regional, həm də qlobal güclərin toqquşan maraqları mütləq nəzərə alınmalıdır. Rəsmi İrəvan, xüsusilə baş nazir Nikol Paşinyan və parlament sədri Alen Simonyan müxtəlif platformalarda Rusiyanın Ermənistana qarşı hibrid metodlardan istifadə etdiyini açıq şəkildə bəyan ediblər. Bildirilib ki, təxribat xarakterli başlıqlar birbaşa Rusiya mediası və bəzi erməni dairələri tərəfindən yaradılır və onlar ən yaxşı halda sonuncunun materiallarını mexaniki şəkildə yenidən çap edirlər. Bundan başqa, hazırda Ermənistan daxilində klan mübarizəsi gedir. Qarabağ klanı adlanan qüvvələr və digər "eks"lər hakimiyyəti ələ keçirməyə çalışırlar. Onlar mətbuatda geniş təbliğ edilir. Kremlin nəzarətindəki media resurslarının yaydığı dezinformasiya, cəmiyyətdə süni qütbləşmə yaratmaq cəhdləri, siyasi sabitliyi pozmağa yönəlmiş addımlar bu çoxölçülü müharibənin görünən tərəfidir.

Təhlükə bununla bitmir. Kiberməkanın dərinliklərində hədəf seçilən dövlət qurumları, bank sektoru və telekommunikasiya infrastrukturu mütəmadi olaraq peşəkar haker qruplarının hücumlarına məruz qalır. İnformasiya sahəsində və beynəlxalq platformalarda Ermənistanın imicinə zərbə vurmaq, daxili auditoriyada dövlətə inamsızlıq toxumu səpmək kimi hibrid alətlər ölkənin suverenliyinə qarşı yönəlib. Seçkiöncəsi dövrdə bu təzyiqlərin daha da intensivləşəcəyi gözlənilir.

Hibrid təhdidlər iqtidar üçün ciddi risklər yaradır, çünki onlar ənənəvi hərbi qarşıdurmadan fərqli olaraq siyasi, informasiya, kiber və psixoloji təsir vasitələrinin paralel istifadəsi ilə dövlətin daxili dayanıqlılığını zəiflətməyə yönəlib. Artıq təkcə texniki boşluqlar deyil, həm də insanların diqqətsizliyi və siyasi həssaslığı birbaşa hədəf alınır. Xüsusilə "@civilcontact.am" kimi saxta domenlərin dövlət rəsmilərinə göndərdiyi məktublar idarəçilikdə xaos yaratmaq və məxfi məlumatları ələ keçirmək məqsədi daşıyır.

Ermənistan Xarici Kəşfiyyat Xidmətinin 2026-cı il üçün hesabatında vurğulandığı kimi, bu fəaliyyətlər sülh prosesinin əhəmiyyətini azaltmaq, cəmiyyətdə "məxfi razılaşmalar" barədə yalan məlumatlar yaymaq və saxta geosiyasi seçimlər təqdim etmək niyyəti güdür. Bu mənzərədə müasir hibrid müharibənin ən qorxulu silahı məhz generativ süni intellekt vasitəsilə yaradılan dezinformasiyadır. Bu səbəbdən iyun ayında keçiriləcək parlament seçkiləri ərəfəsində hibrid təhdidlər və dezinformasiya riski yenidən gündəmin mərkəzinə çevrilib. Bu, nəyi dəyişə bilər?

Suala cavab vermək üçün qeyd edək ki, generativ süni intellekt texnologiyalarından istifadə etməklə ictimai rəyi manipulyasiya etmək və seçki prosesinə dolayı müdaxilə etmək texniki baxımdan daha asan hala gəlib.

***

Hibrid təsir əməliyyatlarının digər təhlükəli istiqaməti kiberfırıldaqçılıq və məlumat oğurluğu ilə bağlıdır ki, burada "taypskvottinq" metodları xüsusi risk amili kimi önə çıxır. Hücum edən tərəflər rəsmi dövlət qurumlarının və ya hakim partiyanın domenlərinə vizual bənzərliyi olan saxta ünvanlar yaradaraq istifadəçiləri aldatmağa çalışırlar. Məsələn, hakim "Mülki müqavilə" partiyası adından istifadə edilərək həyata keçirilən son fişinq hücumları göstərir ki, dövlət rəsmilərinin və seçicilərin diqqətsizliyi artıq strateji hədəfdir. İnsanlar fərqinə varmadan şəxsi məlumatlarını və ya həssas sənədlərə çıxış imkanlarını bu platformalar vasitəsilə ötürürlər. Bu kibermetodlar süni intellektin imkanları ilə birləşdikdə təhlükənin miqyası genişlənir. Generativ süni intellekt artıq real şəxslərin yazı üslubuna, nitq tempinə və emosional çalarlarına uyğun inandırıcı materiallar hazırlamağa qadirdir.

İyun seçkiləri ərəfəsində rəsmi şəxslərin adından yayıla biləcək belə saxta müraciətlər informasiya mühitində sürətli çaşqınlıq yarada, ictimai rəyi yanlış yönləndirə və dövlət institutlarına olan onsuz da kövrək inamı sarsıda bilər. Ermənistan iqtidarı üçün əsas təhdid bu əməliyyatların çoxşaxəli və sinxron xarakteridir. Beləliklə, informasiya manipulyasiyası, sosial şəbəkələrdə psixoloji təsir və siyasi diskreditasiya cəhdləri bir-birini tamamlayan zəncirvari hərəkətə çevrilib. Uzunmüddətli perspektivdə bu fəaliyyətlər təkcə seçki nəticələrinə təsir göstərmək deyil, həm də ölkənin strateji xarici siyasət qərarlarına dolayı müdaxilə etmək, sülh prosesini gözdən salmaq və cəmiyyətdəki emosional həssaslıqlardan istifadə edərək süni geosiyasi seçimlər formalaşdırmaq məqsədi güdür. İyun sınağı Ermənistanın rəqəmsal suverenliyini və institusional dayanıqlılığını qorumaq üçün həlledici dövr olacaq.

Parlament seçkiləri ərəfəsində artan rəqəmsal təhdidləri analiz edən **"Mindsoft" MMC-nin təsisçisi, süni intellekt mütəxəssisi Vüsal Orucov** bildirdi ki, müasir hibrid

müharibələrin ən strateji və kəsərli silahı artıq klassik hərbi texnika deyil, məhz generativ süni intellekt vasitəsilə sistemləşdirilən dezinformasiyadır. Ekspertin qənaətinə görə, iyun seçkiləri ərəfəsində "deepfake" və digər generativ texnologiyalar vasitəsilə dövlət rəsmilərinin adından gerçəklikdən fərqlənməyən saxta video və audio müraciətlərin hazırlanması Ermənistanın daxili sabitliyi üçün ciddi riskdir. V.Orucov vurğuladı ki, bu, cəmiyyətdə idarəolunmaz xaos və panika yaratmaq potensialına malik, texniki cəhətdən hər an icra oluna biləcək bir reallıqdır: "Seçki günü namizədlərin "seçkidən çəkilməsi" və ya "saxta etirafları" ilə bağlı yayıla biləcək inandırıcı süni görüntülər rəsmi təkzib gələnə qədər seçicilərin rəyini geri dönməz şəkildə manipulyasiya edə bilər".

Süni intellekt mütəxəssisi seçki prosesinə təsir göstərə biləcək ən qorxulu amilləri üç əsas istiqamətdə qruplaşdırdı: "İlk növbədə, fərdiləşdirilmiş manipulyasiya (micro-targeting) vasitəsilə hər bir vətəndaşın rəqəmsal profilinə və maraq dairəsinə uyğun saxta xəbər axını yaradıla bilər. Bu metod cəmiyyəti daxildən qütbləşdirərək dövləti xarici müdaxilələrə qarşı müdafiəsiz qoyur. İkinci mühüm amil hücumların koordinasiyalı xarakter daşıması ilə bağlıdır. İnformasiya kirliliyi kiberhücumlar, psixoloji təsir kampaniyaları və siyasi diskreditasiya cəhdləri ilə paralel həyata keçirilir ki, bu da dövlət institutlarının müqavimətini zəiflədir. Nəhayət, aşkarlanma çətinliyi ən böyük problemdir. Alqoritmlərin yaratdığı saxta kontent o qədər inandırıcıdır ki, sıravi seçicinin manipulyasiyanı ayırd etməsi demək olar ki, qeyri-mümkündür".

V.Orucov onu da qeyd etdi ki, iyun seçkiləri Ermənistan üçün təkcə siyasi rəqabət deyil, həm də ciddi texnoloji imtahandır. Ekspertə görə, dövlətin rəqəmsal suverenliyini qorumaq üçün həm institusional islahatların aparılması, həm də cəmiyyətin informasiya savadlılığının artırılması artıq strateji zərurətə çevrilib. Bu rəqəmsal "immun sistemi" qurulmadığı təqdirdə, süni intellekt alətləri demokratik prosesləri daxildən sarsıdan görünməz silaha çevriləcəkdir.

Beləliklə, hibrid təhdidlər təkcə kibertəhlükəsizlik problemi deyil, həm də siyasi institutların dayanıqlılığı, ictimai etimad və informasiya mühitinin sağlamlığı ilə bağlı kompleks təhlükəsizlik çağırışıdır. İyun seçkiləri ərəfəsində dövlət institutlarının, mülki cəmiyyətin və beynəlxalq tərəfdaşların koordinasiyalı fəaliyyəti Ermənistanın institusional dayanıqlılığını təmin etmək və seçki prosesinin bütövlüyünü yeni nəsil təhdidlərdən qorumaq üçün həlledicidir. Yalnız bu halda hibrid təsir əməliyyatlarının yaratdığı sistemli riskləri azaltmaq və dövlətin institusional dayanıqlılığını qorumaq mümkün olacaq.

Pünhan ƏFƏNDİYEV
XQ

Xalq qəzeti.- 2026.- 7 mart (№ 44).- S.1;6.