Hibrid təhdidlərə qarşı mübarizə: COP29 və beynəlxalq təcrübənin - TƏHLİLİ

Müasir dünyada hibrid müharibələr dövlətlərarası qarşıdurmanın yeni forması olaraq ortaya çıxır. Bu hücumlar hərbi gücə əsaslanmasa da, dezinformasiya, hüquqi münaqişələr ("lawfare"), iqtisadi təzyiqlər və kiberhücumlar vasitəsilə hədəfə alınan dövlətin siyasi, iqtisadi və ictimai stabilliyini sarsıtmağa yönəlir. Azərbaycan da beynəlxalq səviyyəli tədbirlər zamanı, xüsusilə COP29 kimi əhəmiyyətli qlobal platformaların təşkilində belə hücumların hədəfi olub.

COP29-a qarşı hibrid hücumlar

Hibrid hücumlar ənənəvi müharibədən fərqli olaraq, çoxşaxəli və qeyri-maddi vasitələrlə icra olunur: Dezinformasiya - Hədəf ölkənin beynəlxalq imicini ləkələmək məqsədilə yalan məlumatların yayılması; "Lawfare" - Hüquqi alətlərin siyasi məqsədlərlə sui-istifadəsi; Sosial media kampaniyaları - Sərfəli rəvayətlər yaratmaq üçün sosial media vasitəsilə ictimai fikrə təsir göstərilməsi; Kiber hücumlar - Dövlətin informasiya sistemlərinə zərbə vuraraq əməliyyat qabiliyyətini zəiflətmək. Hibrid hücumlar yalnız dövlətlər tərəfindən deyil, qeyri-dövlət aktorları, o cümlədən lobbi qrupları, QHT-lər və beynəlxalq media qurumları tərəfindən də həyata keçirilə bilər.

COP29-a qarşı həyata keçirilən dezinformasiya kampaniyaları Azərbaycanın ekoloji təşəbbüslərini nüfuzdan salmaq məqsədini daşıyır. Əsas strategiyalar isə bunlardan ibarətdir - Azərbaycanın təbii resurslardan sui-istifadə etdiyi barədə yalan məlumatların yayılması, Qarabağda ekoloji problemlərin həllində qeyri-səmimi olduğu iddiaları, COP29-un legitimliyini şübhə altına almaq üçün yalan rəvayətlər. Məsələn, erməni diaspor təşkilatları tərəfindən maliyyələşdirilən bəzi beynəlxalq media qurumları, COP29-a qatılmamaq çağırışları ilə çıxış ediblər.

"Lawfare" hücumları - "Lawfare" hüququn siyasi silaha çevrildiyi bir vasitədir. Azərbaycanın COP29 hazırlıqlarına mane olmaq məqsədilə müxtəlif beynəlxalq məhkəmə iddiaları qaldırılıb. Məsələn, bəzi QHT-lər Azərbaycanın insan hüquqlarını pozduğu iddialarını qlobal arenada gündəmə gətirərək ölkəmizin beynəlxalq nüfuzuna zərbə vurmağa çalışıb.

Sosial media platformalarında kampaniyalar - Sosial media, hibrid hücumların ən təsirli vasitələrindən biridir. Məlumatlara görə COP29 ilə əlaqədar 5000-dən çox neqativ həştəq yaradılıb, Azərbaycan əleyhinə troll orduları xüsusi olaraq COP29-a qarşı istifadə edilib.

Erməni lobbisi COP29-a qarşı aparılan kampaniyalarda mühüm rol oynayıb. Onlar maliyyə resurslarını səfərbər edərək, beynəlxalq medianı manipulyasiya ediblər. Həmçinin müxtəlif ölkələrdə

COP29-un əleyhinə siyasi bəyanatların qəbul olunmasını təşviq edib, eyni zamanda, Ermənistan hökuməti ilə birgə koordinasiya edərək beynəlxalq ictimaiyyətdə yanlış təsəvvürlər yaradıb.

Hibrid hücumlara qarşı mübarizədə beynəlxalq təcrübə

Hibrid təhdidlərə qarşı mübarizə aparan dövlətlərdən bəzi nümunələrə nəzər salaq:

Avropa İttifaqı (Aİ), xüsusilə Rusiyanın dezinformasiya kampaniyalarına qarşı "StratCom" vahidi yaradaraq məlumat müharibəsində mübarizə aparır. "East StratCom Task Force" Aİ-nin Şərq Tərəfdaşlığı ölkələrində dezinformasiyaya qarşı mübarizə aparır. Bundan başqa, **NATO** üzv dövlətlərin hibrid hücumlara qarşı hazırlığını gücləndirmək məqsədilə xüsusi proqramlar həyata keçirir. NATO-nun Hibrid Mübarizə Mərkəzi bu istiqamətdə səmərəli strategiyalar tətbiq edir. Həmçinin **Kanada** hökuməti dezinformasiya və sosial media manipulyasiyalarını aşkarlamaq üçün "Digital Citizen Initiative" proqramını tətbiq edir. **Estoniya** 2007-ci ildə genişmiqyaslı kiberhücuma məruz qaldıqdan sonra hibrid hücumlara qarşı mübarizədə qabaqcıl təcrübə əldə edib. NATO-nun Kibermüdafiə üzrə Əməkdaşlıq Mərkəzi (CCDCOE) Estoniyada yerləşir və üzv dövlətlər üçün kibermüdafiə strategiyalarının hazırlanmasında əsas rol oynayır. Eyni zamanda, Estoniya rəqəmsal dövrdə vətəndaş cəmiyyətini məlumatlandırmaq üçün kütləvi maarifləndirmə proqramları həyata keçirir. **Finlandiya** "Hibrid Təhdidlərə qarşı Avropa Mərkəzi"ni (Hybrid CoE) yaratmaqla, Avropa və NATO dövlətləri arasında hibrid mübarizə üzrə əməkdaşlığı gücləndirib. Bu mərkəz məlumat manipulyasiyasını aşkar etmək, kritik infrastrukturun qorunmasını təmin etmək və strateji kommunikasiya üzrə birgə iş aparmaq üçün çalışır. **İsveç** "PsyOps" (Psixoloji Əməliyyatlar) adlanan xüsusi bölmələr vasitəsilə dezinformasiya ilə mübarizə aparır. İsveç hökuməti dezinformasiya kampaniyalarını müəyyənləşdirmək və qarşısını almaq üçün yerli media və vətəndaş cəmiyyəti ilə sıx əməkdaşlıq edir. Bundan başqa, İsveç məktəblərdə media savadlılığını tədris edərək gənclərin kritik düşünmə bacarıqlarını inkişaf etdirir. **Avstraliya** hökuməti "Critical Infrastructure Centre" vasitəsilə milli infrastruktura qarşı hibrid hücumların qarşısını almağa fokuslanıb. Bundan əlavə, "Foreign Interference Taskforce" (Xarici Müdaxilə Əleyhinə Qüvvə) xarici təsirlərə və dezinformasiyaya qarşı ölkə daxilində koordinasiyanı gücləndirir. **ABŞ** "Countering Foreign Influence Task Force" vasitəsilə seçkilərə xarici müdaxiləyə və dezinformasiyaya qarşı mübarizə aparır. FBI və DHS (Department of Homeland Security) məlumat mübadiləsini asanlaşdırmaq və ictimaiyyəti xəbərdar etmək üçün xüsusi proqramlar hazırlayır. Həmçinin "Cybersecurity and Infrastructure Security Agency" (CISA) kritik infrastrukturun qorunmasını təmin edir. **Ukrayna** davamlı hibrid hücumlara qarşı mübarizə aparmaq üçün "StopFake" adlı qeyri-hökumət təşəbbüsünü işə salıb. Bu platforma dezinformasiyanın ifşa olunması və təhlilini həyata keçirir. Bundan əlavə, Ukrayna "Cyber Rapid Response Teams" (CRRT) vasitəsilə

kiberhücumlara sürətli cavab vermək üçün regional əməkdaşlıq edir. **Böyük Britaniya** "National Cyber Security Centre" (NCSC) vasitəsilə milli təhlükəsizliyə yönəlmiş kiberhücumlara qarşı mübarizəni gücləndirib. Bundan əlavə, "Resilience Against Influence Operations" proqramı xarici dezinformasiya kampaniyalarına qarşı dövlət və ictimai sektor arasında koordinasiyanı inkişaf etdirir.

Bu beynəlxalq təcrübələr göstərir ki, hibrid təhdidlərə qarşı mübarizədə səmərəli olmaq üçün beynəlxalq əməkdaşlıq, informasiya texnologiyalarından istifadə və cəmiyyətin məlumatlılıq səviyyəsinin artırılması əsas amillərdəndir.

Azərbaycan təcrübəsi və tövsiyələr

Azərbaycanın COP29-a qarşı hibrid hücumlarla mübarizəsi həm milli, həm də beynəlxalq səviyyədə koordinasiya tələb edir. Buna əsasən müəyyən tövsiyələrə riayət etmək lazımdır. Belə ki, dezinformasiyaya qarşı mübarizədə milli səviyyədə strateji kommunikasiya mexanizmlərinin gücləndirilməsi əhəmiyyətlidir. Həmçinin beynəlxalq əməkdaşlıq da burada mühüm əhəmiyyət kəsb edir. İnformasiya təhlükəsizliyində - kiberhücumlara qarşı milli müdafiə mexanizmlərinin inkişaf etdirilməsi vacibdir. Qlobal maarifləndirmə prosesi - COP29-un əhəmiyyətini beynəlxalq ictimaiyyətə səmərəli şəkildə çatdırmaq üçün PR strategiyalarının qurulması mühüm amillərdəndir.

COP29 ətrafında həyata keçirilən hibrid hücumlar, təkcə Azərbaycanın deyil, bütövlükdə beynəlxalq ictimaiyyətin ekoloji təşəbbüslərinə yönəlmiş təhdidlərdir. Bu təhdidlərə qarşı mübarizə yalnız güclü milli strategiyalar deyil, həm də beynəlxalq həmrəyliyin möhkəmləndirilməsini tələb edir. Azərbaycan hibrid hücumların öhdəsindən gəlmək üçün həm milli informasiya təhlükəsizliyini gücləndirməli, həm də beynəlxalq dəstək mexanizmlərindən faydalanmalıdır. COP29 yalnız ekoloji tədbir deyil, həm də Azərbaycanın qlobal ekoloji problemlərin həllində liderlik potensialını göstərən platformadır.

AZƏRTAC
2024, 25 dekabr