Documente declasificate din CSAT⁄ România - tinta pentru actiuni hibride ruse; campania lui Georgescu - finantata

Informatiile prezentate de Serviciul Român de Informatii, Serviciul de Informatii Externe si Ministerul Afacerilor Interne în cadrul sedintei Consiliului Suprem de Aparare a Ţarii (CSAT) din data de 28 noiembrie care au fost declasificate, miercuri, de presedintele Klaus Iohannis indica faptul ca finantarea campaniei candidatului independent Calin Georgescu pe TikTok s-a ridicat la un milion de euro, ca au avut loc actiuni ale unui actor cibernetic statal asupra infrastructurilor IT&C suport pentru procesul electoral si ca România este o tinta pentru actiuni hibride agresive ruse.

Presedintele Klaus Iohannis a fost de acord cu declasificarea informatiilor, potrivit legii, la solicitarea institutiilor emitente.

***

În documentul declasificat, **SRI** arata ca finantarea campaniei lui Calin Georgescu pe TikTok a fost realizata de Bogdan Peschir si s-a ridicat la un milion de euro.

"Acesta, utilizând contul 'bogpr', a realizat donatii pe TikTok de peste un milion de euro. Dupa ce a devenit subiect de dezbatere publica, implicarea 'bogpr' în finantarea promovarii lui Calin Georgescu la nivelul platformei a fost confirmata inclusiv de reprezentantii TikTok în dialogul cu autoritatile române în data de 28 noiembrie 2024", arata SRI.

Reprezentantii TikTok au confirmat identitatea utilizatorului "bogpr" si au mentionat ca acesta a efectuat plati în valoare de 381.000 de dolari, în perioada 24 octombrie - 24 noiembrie 2024, catre utilizatori ai unor conturi de TikTok implicati în promovarea candidatului Calin Georgescu, inclusiv dupa data încheierii campaniei electorale, puncteaza SRI.

SRI arata ca finantarea influencerilor TikTok a fost asigurata prin platforma FameUp (dedicata monetizarii activitatilor de promovare în mediul online), la nivelul careia a fost publicata oportunitatea de reclama, alaturi de descrieri bine definite. "Una dintre metodele de atragere la colaborare a influencerilor români pentru promovarea candidaturii lui Calin Georgescu a fost contactarea pe e-mail a acestora de firma (...), de origine sud-africana, care oferea suma de 1.000 de euro pentru distribuirea unui videoclip realizat de acestia", arata SRI.

Sursa citata apreciaza ca în contextul primului tur al alegerilor prezidentiale au fost obtinute date care au relevat "o campanie de promovare agresiva, derulata cu eludarea legislatiei nationale în domeniul electoral, dar si exploatarea algoritmilor unor platforme de social media pentru cresterea în ritm accelerat a popularitatii lui Calin Georgescu".

În acest sens, arata SRI, a fost utilizata platforma TikTok. Activitatea de promovare masiva a presupus o campanie pe TikTok, prin intermediul mai multor conturi coordonate ce au publicat activ continut electoral, atât cu ajutorul algoritmilor de recomandare, cât si prin promovare platita.

Reteaua de conturi asociata direct campaniei lui Calin Georgescu a fost formata initial din 25.000 de conturi la nivelul platformei TikTok, care au devenit foarte active cu doua saptamâni înaintea datei scrutinului electoral. Campania de promovare a avut o organizare deosebit de buna, numarul urmaritorilor crescând semnificativ.

A fost identificat canalul de Telegram Propagator - implica-te si tu, Renasterea României, Hrana Apa Energie (Gpropagatorcg), care are rol de a coordona alti utilizatori cu privire la postarile si continutul video distribuit.

"Abonatii @propagatorcg au primit instructiuni clare privind modalitatea de actiune a conturilor, recomandari privind comportamentul utilizatorilor la nivelul TikTok, respectiv mesajele care ar fi urmat sa fie promovate sau distribuite, în sensul includerii unor emoji special alese si a numelui candidatului pentru a exploata algoritmii TikTok. Acestea erau pregatite anterior si încarcate instant în cadrul TikTok", mai arata SRI.

În activitatea de promovare a lui Calin Georgescu a fost utilizata o retea extinsa de persoane publice cu notorietate ridicata de la nivelul platformei TikTok (influenceri), prin intermediul carora si-a promovat campania atât în mod direct (prin sustinerea publica a candidatului), cât si indirect (prin mesaje aparent neutre, dar care contineau etichete asociate candidatului, precum #echilbrusiverticalitate). În mod intentionat, o parte dintre acestia nu au marcat publicitatea ca fiind platita, pentru a evita asocierea postarilor cu cele dedicate campaniilor electorale.

De asemenea, potrivit sursei citate, au fost create si utilizate conturi care reprezinta în fals institutii ale statului român, precum conturi TikTok care au utilizat în fals sigla SRI si titulatura Brigada Antiterorista (BAT), respectiv afisau mii de urmaritori si peste 100.000 de like-uri.

Pe aceste conturi au fost distribuite numeroase imagini cu fortele Politiei Române si BAT, preluate din spatiul public. La comentarii au fost identificate postari apreciative la adresa SRI-BAT/ institutiilor de forta si de sustinere a candidatului Calin Georgescu, inducând astfel, în fals, ideea ca institutiile statului îl sustin pe acesta.

Pe 20 noiembrie, precizeaza SRI, BEC a dispus "înlaturarea materialelor de propaganda electorala din mediul online ce îl ilustreaza pe candidatul Calin Georgescu la alegerile pentru Presedintele României din anul 2024, care nu contin codul de identificare al mandatarului fiscal".

Solicitarea a fost transmisa catre TikTok, prin intermediul AEP, în data de 21 noiembrie.

A doua zi, TikTok a transmis AEP confirmarea eliminarii postarilor care fac obiectul deciziei BEC, prin blocarea accesului vizual la acestea de pe teritoriul României, ele ramânând vizibile în alte state si putând fi distribuite.

"Cu toate acestea, verificarile ulterioare au relevat ca TikTok nu a sters continutul electoral conform solicitarii AEP, iar acesta a continuat sa fie disponibil publicului din România, chiar si dupa încheierea campaniei electorale, inclusiv în ziua alegerilor (aspecte ce contravin legislatiei române)", puncteaza SRI.

SRI arata ca postarile cu continut pur electoral ale conturilor asociate retelei care îl promoveaza pe Calin Georgescu au fost catalogate de TikTok ca postari de divertisment.

Într-un alt document al SRI se precizeaza ca au avut loc actiuni ale unui actor cibernetic statal asupra infrastructurilor IT&C suport pentru procesul electoral, gazduite de AEP si STS.

"Prin metode specifice, în data de 24.11.2024, SRI a obtinut date cu privire la publicarea unor credentiale de acces asociate "bec.ro", "roaep.ro" si "registrulelectoral.ro" în cadrul unor platforme de criminalitate cibernetica de sorginte rusa, date similare fiind identificate si în cadrul unui canal privat de Telegram recunoscut pentru diseminarea de date exfiltrate din foarte multe state, mai putin Federatia Rusa. În urma verificarilor demarate s-a stabilit ca exfiltrarea s-a realizat fie prin targetarea utilizatorilor legitimi catre care au fost distribuite credentialele de tip utilizator/parola, fie prin exploatarea serverului legitim de instruire pus la dispozitie de catre STS la adresa https://operatorsectie.roaep.ro", mentioneaza SRI.

Aceste postari au fost efectuate dupa ce pe 19 noiembrie un incident cibernetic a targetat si a afectat infrastructura IT&C a AEP, în urma caruia atacatori cibernetici au compromis un server de harti (gis.registrulelectoral.ro), conectat atât în exterior, la internet, cât si la reteaua interna a AEP.

"În context, a fost identificat un numar ridicat de atacuri cibernetice (peste 85.000), care au vizat exploatarea vulnerabilitatilor existente la nivelul sistemelor informatice de suport pentru procesul electoral, în vederea obtinerii accesului la datele din sistemele informatice, alterarii integritatii acestora, schimbarii continutului prezentat publicului larg si indisponibilizarii infrastructurii", precizeaza SRI.

SRI mentioneaza ca aceste atacuri au continuat într-un mod sustinut, inclusiv în ziua alegerilor si în noaptea post alegeri si ca, pentru lansarea atacurilor, au fost utilizate sisteme informatice din peste 33 de tari, folosind metode de anonimizare avansate pentru a îngreuna procesul de atribuire.

Sursa citata subliniaza ca au fost demarate investigatii specifice împreuna cu AEP si STS.

"Întrucât evaluarea cu privire la atacul cibernetic este în derulare, în prezent nu detinem date certe cu privire la atacator ori cu privire la afectarea procesului electoral", indica SRI.

***

SIE arata ca România, alaturi de alte state de pe Flancul Estic al NATO, "a devenit o prioritate pentru actiunile ostile ale Rusiei, existând un interes în crestere la Kremlin pentru a influenta (cel putin) mood-ul si agenda în societatea româneasca în context electoral".

Aceste actiuni, arata SIE, se manifesta prin propaganda si dezinformare, sprijinirea unor candidati eurosceptici si alimentarea unor miscari antisistem, inclusiv prin "implicarea acestora în proteste care sa modeleze agenda publica", încurajarea nemultumirilor/provocarea de reactii emotionale la nivelul populatiei, astfel încât sa puna presiune pe autoritati sa reduca/stopeze sprijinul pentru Ucraina.

"Apreciem ca România este o tinta pentru actiuni hibride agresive ruse, inclusiv atacuri cibernetice si scurgeri de informatii (hacks and leaks) si sabotaje", afirma SIE.

În documentul înaintat CSAT, SIE a informat ca "situatia politica din România a fost abordata si în cadrul talk-show-urilor politice din Rusia - jurnalistii rusi lanseaza ideea ca fortele pro-ruse din România ar putea obtine peste 30% la alegerile parlamentare".

Analiza modului în care aparatul de propaganda rusa a vizat România în 2024 include mesaje care au vizat: (I) divizarea societatii pe teme precum controlul exercitat de SUA/NATO asupra României, amenintarile de securitate generate de statutul de membru NATO si de sprijinul acordat Kievului; (II) discreditarea capacitatii de raspuns a NATO si României, amplificarea neîncrederii populatiei în capacitatea de aparare nationala; (III) erodarea sprijinului populatiei pentru deciziile de politica externa ale României; (IV) evidentierea implicarii României în conflict si ambitiilor teritoriale în raport cu statele vecine (ex. Ucraina si R. Moldova).

***

În documentul prezentat de **MAI** - Directia Generala de Protectie Interna se arata ca verificarile tehnice de specialitate în mediul online si analiza valorilor metrice identificate în social media, preponderent pe platforma TikTok, în procesul electoral, au validat existenta unei campanii electorale neetichetate ca atare, în care, începând cu luna noiembrie, un numar de peste 100 de influenceri (care numarau în total peste 8 milioane de urmaritori activi) au fost supusi unei actiuni de manipulare în privinta identitatii candidatului promovat.

Sursa citata precizeaza ca TikTok nu a implementat instructiunile BEC privind marcarea drept candidat politic, respectiv marcarea materialelor electorale de tip video cu codul unic atribuit de AEP fiecarui candidat.

De asemenea, indica faptul ca analiza metrica a relevat o crestere abrupta în intervalul 13 - 26 noiembrie, ajungând pe locul noua la nivel mondial în topul trendurilor de promovare a continutului video asociat mai multor hashtag-uri utilizate în campania electorala a lui Calin Georgescu, însa nu a fost identificata o amplificare artificiala la nivelul platformei TikTok pâna în data de 24 noiembrie, explozia numarului de vizualizari, de ordinul sutelor de milioane, fiind înregistrata ulterior datei de 25 noiembrie.

Datele analizate de MAI au relevat aproximativ 130 de conturi TikTok prin intermediul carora au fost diseminate video-uri cu un astfel de continut, utilizând hashtag-urile #echilibrusiverticalitate, #prezidentiale2024, #unliderpotrivitpentrumine, majoritatea postarilor de acest tip nefiind marcate ca reclame platite.

"Evaluarea scenariului utilizat pentru realizarea elementelor de continut indica situatii similare realizate în cadrul unor actiuni de influentare a intentiei de vot din Republica Moldova. În concret, o parte din textul de început utilizat de influenceri români pentru promovarea candidatului prorus din Republica Moldova a fost regasit în cadrul postarilor mentionate. În cadrul sectiunii de comentarii aferente fiecarui element de continut au fost identificate o serie de mesaje de promovare a unui candidat la prezidentiale. Analiza acestor conturi indica anomalii în constituirea acestora, existând indicii privind utilizarea unor conturi fictive create doar pentru distribuirea de astfel de comentarii", se mentioneaza în documentul MAI, unde se precizeaza ca majoritatea influencerilor nu au cunoscut faptul ca promoveaza un candidat anume.

Se precizeaza ca influencerii au fost platiti si ca în cazul de fata baza de calcul pentru o astfel de campanie se plateste cu 400 lei pentru 20.000 de urmaritori.

"Unii dintre sustinatorii campaniei implicati în promovarea si cumpararea de voturi sunt exponenti ai mediilor extremiste de dreapta, infractionale si ai cultelor religioase, implicate anterior în promovarea unor narative proruse, antisemite, anti-NATO sau împotriva Ucrainei", mai arata MAI, dând ca exemplu pe liderul unui clan.

***
Serviciul de Telecomunicatii Speciale arata ca în perioada desfasurarii procesului electoral au fost identificate atacuri cibernetice de tip DDOS la nivelul infrastructuri IT&C, precum si la nivelul altor resurse din sfera guvernamentala. Atacurile la adresa infrastructurilor IT&C gestionate de STS au fost blocate cu succes, iar pentru celelalte au fost informati administratorii de sistem din cadrul institutiilor afectate.

La nivelul sistemelor de securitate cibernetica proprii nu au fost identificate indicii cu privire la compromiterea datelor aferente procesului de votare din SIMPV si SICPV, subliniaza STS.

Totodata, pentru pregatirea procesului electoral, la nivelul Serviciului de Telecomunicatii Speciale s-au desfasurat procese de identificare a amenintarilor, evaluare a vulnerabilitatilor, analiza riscurilor, configurarea sigura, testarea de securitate cibernetica, precum si implementarea masurilor pentru asigurarea detectiei, protectiei, raspunsului si recuperarii în cazul incidentelor de securitate cibernetica.

STS afirma ca a implementat, astfel, masuri tehnice de detectie si protectie împotriva atacurilor cibernetice, inclusiv a celor complexe tip APT, prin utilizarea unei solutii, operationalizata si gestionata exclusiv la nivelul STS, care permite verificarea configuratiilor sigure pe toate sistemele, detectia activitatilor malitioase, detectia ransomware, monitorizarea integritatii fisierelor din sistemele informatice, detectia vulnerabilitatilor, analiza integrata si corelarea jurnalelor de securitate, precum si identificarea amenintarilor.