ROMANIAN INTELLIGENCE SERVICE

NOTE NO. 2 TO THE ROMANIAN SUPREME COUNCIL FOR NATIONAL DEFENSE

I. **Actions of a cyber state actor** on the IT&C infrastructures supporting the electoral process, hosted by the Permanent Electoral Authority (AEP) and the Special Telecommunications Service (STS).

By using specific methods, on 24.11.2024, the Romanian Intelligence Service (SRI) obtained data regarding the publication of access credentials associated with "**bec.ro**" (i.e. Romanian Central Electoral Office – BEC - website), "**roaep.ro**" (i.e. AEP website) and "**registrulelectoral.ro**" (i.e. Romanian Electoral Registry/AEP website) within several Russian origin cybercrime platforms, similar data being also identified within a private Telegram channel well known for disseminating exfiltrated data from many states, except the Russian Federation.

Following the investigations initiated, it was determined that the exfiltration was carried out either by targeting legitimate users to whom the user/password credentials were distributed, or by exploiting the legitimate training server made available by STS at **https://operatorsectie.roaep.ro**.

Regarding the infrastructure topology, STS manages the main sequence related to the voting process: recording voter turnout, ensuring the accuracy of ballot counting by video recording the process of opening the ballot boxes and counting the votes, and centralizing the results.

The infrastructure sequence managed by AEP serves the real-time display of voter turnout, statistics on vote distribution by various criteria (categories, age, gender, urban/rural environment, etc.), as well as making the electoral legislation available.

These posts were published after a cyber incident targeted and affected the AEP IT&C infrastructure on 19.11.2024, through which cyber attackers managed to compromise a map server (***gis.registrulelectoral.ro***), connected both externally, to the internet, and to AEP's internal network.

In this context, **a large number of cyber-attacks**[1] **(over 85,000)** were identified, which aimed to exploit existing vulnerabilities in the IT systems supporting the electoral process, to **gain access to data in the IT systems, alter their integrity, change the content presented to the public and make the infrastructure unavailable**.

The National Cyberint Center conducted technical assessments on related information systems by analysing the log files for the period 20-26.11.2024, generated by the cybersecurity equipment used by:

- *prezenta.roaep.ro* - platform for monitoring and displaying statistics on voter turnout;
- *voting_roaep.ro* - blockchain transaction platform;
- *prezidentiale1-sicpv.bec.ro* - computer system for centralizing minutes;
- *simpv.bec.ro* - computer system for monitoring voter turnout;
- *simpv.roaep.ro* - computer system for monitoring voter turnout;
- *simpv.stsnet.ro* - computer system for monitoring voter turnout.

[1] 1 Type:
- SQL injection (SQLi) - Attack that involves injecting SQL-type malicious code into an application to access and/or modify the database behind it;
- Cross Site Scripting (XSS) - Attack that exploits a vulnerability found in a web page and allows an attacker to insert lines of code into web pages visited by other users (victims), to obtain data with restricted access.

The attacks in question continued in a **sustained manner, including on election day and the night after the election (25.11.2024). Computer systems from over 33 countries** were used to launch the attacks, using advanced anonymization methods to make the attribution process difficult.

* It must be underlined that specific investigations have been launched together with the AEP and STS. As the assessment of the cyberattack is ongoing, we currently do not have any clear data on the attacker or on the impact on the electoral process.

The modus operandi, as well as the scale of the cyber campaign, lead to the conclusion that the attacker has considerable resources that are **correlated with specific methods used by a state-sponsored attacker**. At the same time, the AEP infrastructure remains affected by vulnerabilities which, to the extent that they are exploited by attackers, can escalate access within the network and ensure persistence.

II. In the context of the issues circulating in the online environment, the obtained data revealed that the reason for the massive and accelerated growth of **Călin GEORGESCU**'s popularity on the TikTok social platform is due to a very well-organized promotional campaign.

Călin GEORGESCU benefited from preferential treatment on the TikTok platform, because the content he posted **was not marked as belonging to a candidate**, which favoured mass dissemination, as the published videos were not officially associated with the electoral campaign.

Consequently, **his visibility increased preferentially compared to the other candidates, whose posts were massively filtered, exponentially diminishing their online presence**.

This preferential treatment was exacerbated by **TikTok's failure to comply with BEC Decision** no. 175D of 20.11.2024, which, in art. 3, ordered "the removal of electoral propaganda materials from the online environment that illustrate the candidate Călin Georgescu in the 2024 Romanian Presidential elections, which do not contain the identification code of the fiscal representative".

The request was sent to TikTok, through AEP, on 21.11.2024, 08:00 hrs. Subsequently, at TikTok's request, a return was made with the CMF code, which following the analysis made by AEP was not found in any of the candidate's posts.

On 22.11.2024, 13:47 hrs, TikTok sent AEP confirmation of the removal of the posts that are the subject of BEC Decision no. 175D of 20.11.2024, by blocking visual access to them from the territory of Romania, **they still remaining visible in other states and being possible to be distributed**.

Meanwhile, according to information obtained from TikTok representatives, an analysis was carried out regarding the online activities subsumed under the Călin GEORGESCU promotion campaign.

TikTok's first notification of the fact that a Călin GEORGESCU promotion campaign was underway took place in 2020, and in 2021, it was reported by them (most likely to TikTok management) as a suspicious activity.

The conclusions of the current analysis reveal the following:

• Telegram and Discord channels were discovered where they discussed how to coordinate and

avoid being blocked on the platform, so no direct link was identified between the multiple TikTok accounts used to promote Călin GEORGESCU, given that the activity was carried out from multiple geolocations;

• **the activity of the accounts was allegedly coordinated by a state actor**, who would have used an alternative communication channel to "roll" messages on the platform;

• does not use bot farms on the platform, but operates more discreetly from the outside, so as not to violate the platform's usage policies;

• those involved in the campaign to promote the person in question demonstrate a very good knowledge of TikTok's security policies, and have the necessary know-how to circumvent them;

• there is a very good digital marketing company behind it;

• the social accounts that promoted Călin GEORGESCU on TikTok disseminated identical messages, without any coordination on the platform (no fingerprints were detected that would connect the devices used);

The growth of accounts was not organic (similar to natural viral events), so TikTok believes that they are basically coordinated volunteers ("**mass guerrilla political campaign**" or "**brute force attack in cybersecurity**").

• the dissemination of messages within the TikTok platform was carried out in swarms (swarming).

Also, during the last days, TikTok has identified a massive promotional activity, carried out in the last two weeks, in support of POT (Young People's Party), a sovereigntist party, founded in 2023, which supports Călin GEORGESCU.