

**Alliance
4Europe**



Persistent Infrastructure and Cross-Border Influence Operations Targeting European Elections on X

Authors

Maria Voltsichina, Alliance4Europe
Robert van der Noordaa, Trollrensics

Persistent Infrastructure and Cross-Border Influence Operations Targeting European Elections on X

Authors:

Maria Voltsichina - Alliance4Europe

Robert van der Noordaa - Trollrensics

Introduction

This investigation was initiated by [HEIO](#) (Hybrid Election Integrity Observatory). The project was funded by [SIDN fonds](#), and the [Democracy and Media Foundation](#). Within the HEIO consortium, [Trollrensics](#), in cooperation with the media company [RTL](#), focused on identifying coordinated inauthentic networks during the 2025 elections, commonly referred to as troll farms. The methodology employed involved mapping retweet patterns of high-engagement posts on X (formerly Twitter) relating to the Dutch elections. As a result of that research effort, RTL Nieuws and Trollrensics [identified over 550 fake accounts on X](#) that actively amplified politically charged and socially divisive content in the lead-up to and following the Dutch parliamentary elections of 29 October 2025. The accounts were predominantly operated from West African countries, with at least 225 traceable to Nigeria and a significant additional cluster originating from Ghana and other West African and Asian nations. In the onset of the Hungarian elections in April 2026, Trollrensics noticed an overlap with the same assets used during the Dutch elections amplifying election related content on X in Hungary. The same assets were identified to use an identical modus operandi to influence X recommendations algorithm to boost pro-Orbán and pro-Russian content. In collaboration with Trollrensics, Alliance4Europe analysed scraped data behind accounts boosting political content on X.

Modus Operandi during the Dutch Elections 2025

This network, initially [discovered](#) during the Dutch 2025 elections, has been flagged due to its distinctive modus operandi. The assets within this network employed two primary amplification techniques. The first was mass retweeting: the 550 identified accounts generated over 23,000 posts

since October 2025, the vast majority of which were retweets of Dutch-language political content, also [aiming](#) to influence the Dutch elections. Content was heavily skewed toward far-right and anti-institutional narratives, with Forum for Democracy (FvD) [receiving the highest volume of amplification](#), followed by Geert Wilders and PVV. The second technique was the mass following of small, hyperactive accounts: rather than targeting high-profile politicians or parties, the network disproportionately followed smaller, anonymous accounts with strongly polarising content. This behaviour artificially inflated the apparent follower counts and social credibility of these accounts, potentially triggering X's recommender algorithm to surface their content more widely. Both likes and retweets are well-established vectors through which content can be artificially amplified to trending status. Through this mapping exercise, a significant number of anomalous accounts were rapidly identified.

These accounts displayed inconsistent characteristics: some carried Dutch-language bios, names and handles, while others featured English-language profiles with listed locations in the United States despite focusing on Dutch content, raising immediate flags regarding their authenticity and origin. A subset of the identified accounts was designed to appear authentically Dutch, featuring Dutch-language bio's, Dutch names, and activity consisting predominantly of retweeting Dutch-language content. However, the majority of active accounts were found to be either repurposed MAGA-affiliated accounts or components of broader foreign coordinated networks. The stated location origins of these networks span multiple countries across West Africa and Southeast Asia, specifically: Nigeria, Benin, Ivory Coast, Ghana, Gambia, Thailand, Hong Kong, and Vietnam.

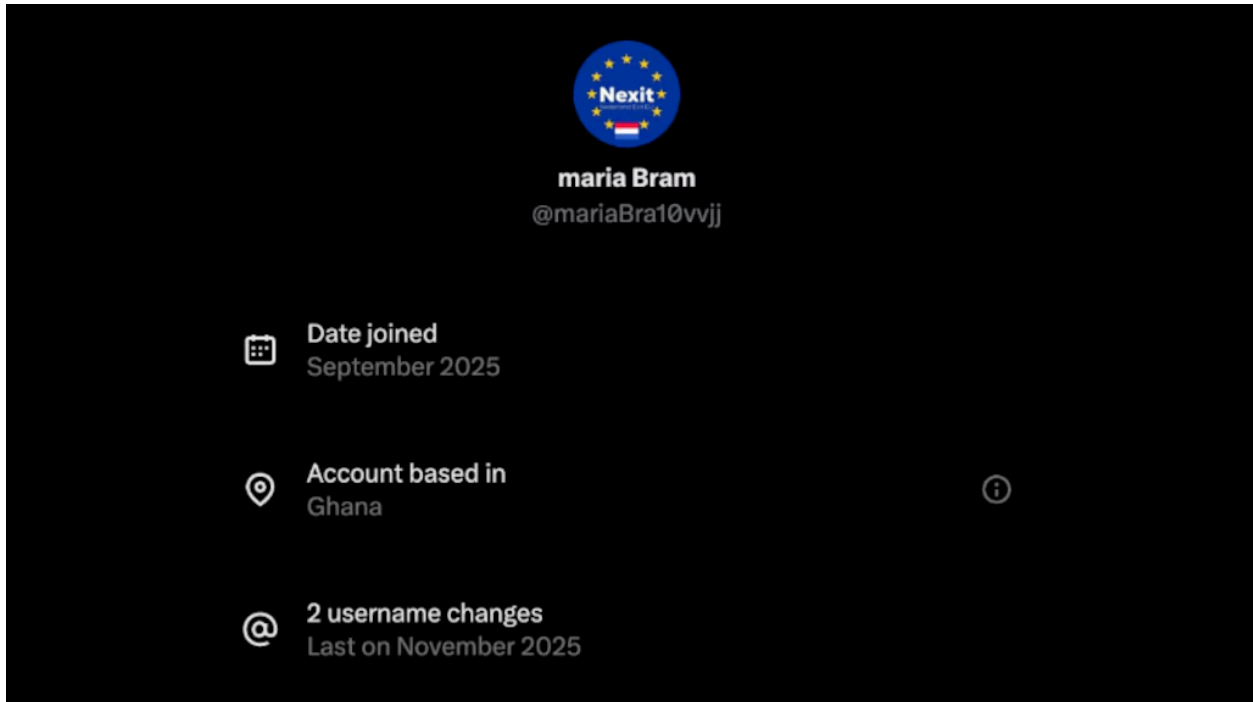


Fig. 1: the location on one of the identified accounts found to be engaging in boosting Dutch right-wing content ahead of the Dutch elections, listed as Ghana. Credits: RTL & Trollensics Reporting.

The accounts were constructed to mimic Dutch users, employing Dutch names, Dutch-language bio's, and shared content written in Dutch. However, [several indicators pointed to their inauthenticity](#), including non-existent Dutch first names, unconventional capitalisation, and bursts of activity, in some cases dozens of retweets within a span of minutes. Names of [prominent Dutch public figures](#) were also appropriated for fake profiles, including those of musician André Rieu, actress Karin Bloemen, speed skater Jutta Leerdam, and former politician Henk Otten. Accounts were observed changing their names, usernames, and profile pictures during the investigation, suggesting active operational management.

As an illustrative example, dozens of accounts impersonating or mimicking the identity of *Laurine Hayven* were detected.

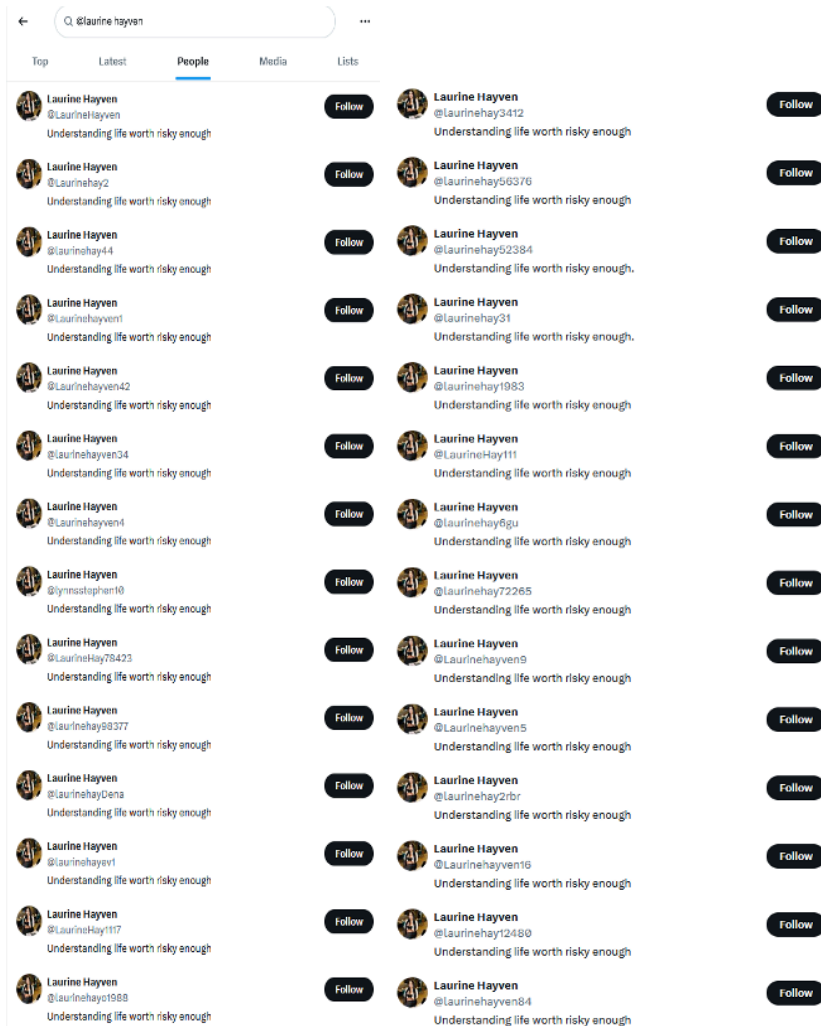


Fig. 2 & 3: The active accounts on X that identically imitated Laurine Hayven and were involved in amplification of polarising political content.

RTL Nieuws [identified](#) 204 accounts followed by more than 50 fake accounts, and established that for 161 accounts, the majority of their followers consisted of fake profiles. Analysts noted that the true scale of the network is likely considerably larger, with hundreds of additional unidentified accounts displaying similar behavioural patterns. While the AIVD, the Dutch domestic intelligence agency, [stated](#) it had no evidence of a large-scale state-sponsored campaign specifically targeting the Netherlands, multiple independent experts assessed Russian involvement as probable. Troll farm operations in West Africa have [previously been linked to Russian actors](#). The network's preferential amplification of pro-FvD content, whose leader Thierry Baudet has fallen into [controversy over alleged ties to Russia](#) due to [exposed messaging history](#), appearances [on sanctioned media](#), and its positions on arms deliveries to Ukraine, was [cited](#) as a directional indicator.

In response to the investigation, X began suspending a portion of the identified accounts in the weeks following publication, though the majority of the identified accounts remained active at the time of our secondary investigation. The Netherlands Authority for Consumers and Markets deferred oversight responsibility to the European Commission, which confirmed an ongoing investigation into whether X had done enough to protect the integrity of European elections.

Coordinated Inauthentic Behaviour (CIB) Network’s Reusability

The network, identified ahead of the Dutch elections, was once again flagged ahead of another European election period. Flagged by Trollrensics, the same accounts seemed to have switched focus to cover the Hungarian elections in late March and beginning of April 2026. The accounts used the same modus operandi to amplify pro-Russian, anti-establishment and pro-Orbán content. One of the primary indicators pointing to this pattern was the observation that a number of accounts within the initial Nigerian network active in the Netherlands were following large volumes of Hungarian accounts. Notably, several of the previously identified Laurine Hayven impersonation accounts were found to be following Hungarian language profiles, providing a link between the coordinated inauthentic accounts and the pro-Orbán/pro-Russian Hungarian content ecosystem.

laurinehay3412	Laurine Hayven	2025-08-1	147	5322	-1	294 "Nigeria"
laurinehay37632	Laurine Hayven	2025-08-1	160	6239	-1	525 "Nigeria"
laurinehay49822	Laurine Hayven	2025-07-0	163	6253	-1	616 "Nigeria"
laurinehay89243	Laurine Hayven	2025-08-1	176	5776	-1	402 "Nigeria"
laurinehay98377	Laurine Hayven	2024-12-2	199	2837	-1	67 "Nigeria"
laurinehayev1	Laurine Hayven	2025-03-1	196	3048	-1	78 "Nigeria"
laurinehayMann	Laurine Hayven	2013-11-0	539	2521	-1	191 "Nigeria"
laurinehayo1988	Laurine Hayven	2025-07-1	158	4921	-1	386 "Nigeria"
laurinehayvemon	Laurine Hayven	2012-12-2	443	1981	-1	729 "Nigeria"

Fig. 4: Laurine Hayven accounts following the selected Hungarian accounts.

The Hungarian Branch

The research was structured across three sequential phases. Phase 1 initiated the data collection by mapping the followers and following lists of two categories of accounts: accounts belonging to the previously identified networks in the Netherlands (such as those geolocated to Nigeria) that were observed following Hungarian accounts, and Hungarian accounts that appeared to be systematically targeted by these networks (i.e. systematically followed and reposted from).

Phase 2 built on this foundation by isolating the network accounts originating from Nigeria within the dataset assembled in Phase 1, and subsequently collecting the followers and following lists of those accounts.

Phase 3 was designed to deepen the understanding of the network’s operational structure and to produce a more accurate estimate of its scale. The followers and following lists of 21 Nigerian network accounts (all of which had been observed following Hungarian accounts) were collected. From the full set of accounts followed by these 21 accounts, a query was constructed to identify which Hungarian accounts were most frequently followed across the network. The start of data collection for Hungary was that Trollrensics mapped followers and following of 2 types of accounts. Type one is an account belonging to the networks (Nigeria etc) which follows Hungarian accounts, depicted in Fig. 5, and type two, which are Hungarian accounts which seems to be followed by the accounts located in the initial investigation depicted in Fig. 6.

Platform	Type	Searchstring	Enabled	Last Run	Created		
X x	user	AzaraYucil70847	✓	1 day ago	2026-04-06 17:53	Profile	Edit
X x	user	AzaraYucil162292	✓	1 day ago	2026-04-06 20:58	Profile	Edit
X x	user	Azarayucil9127	✓	1 day ago	2026-04-06 21:09	Profile	Edit
X x	user	MichaelBen38631	✓	1 day ago	2026-04-07 10:11	Profile	Edit
X x	user	MoynihanBr36525	✓	1 day ago	2026-04-07 10:29	Profile	Edit
X x	user	camerondai12	✓	1 day ago	2026-04-07 10:52	Profile	Edit
X x	user	doge_usda_	✓	1 day ago	2026-04-07 14:15	Profile	Edit
X x	user	Hakanaran123357	✓	1 day ago	2026-04-07 15:02	Profile	Edit
X x	user	Jasonmomoa59849	✓	1 day ago	2026-04-07 15:14	Profile	Edit
X x	user	KNatassh	✓	23 hours ago	2026-04-07 15:40	Profile	Edit
X x	user	realjakobzoli	✓	23 hours ago	2026-04-07 15:45	Profile	Edit
X x	user	spaceX1074	✓	23 hours ago	2026-04-07 16:17	Profile	Edit
X x	user	szabarine1806	✓	23 hours ago	2026-04-07 16:18	Profile	Edit
X x	user	tiborradicsfx	✓	21 hours ago	2026-04-07 17:30	Profile	Edit
X x	user	VeriaStell86789	✓	21 hours ago	2026-04-07 17:34	Profile	Edit
X x	user	wrawniwil	✓	21 hours ago	2026-04-07 17:36	Profile	Edit
X x	user	pauITzalesky	✓	21 hours ago	2026-04-07 17:44	Profile	Edit
X x	user	olamidotun2025	✓	19 hours ago	2026-04-07 19:44	Profile	Edit
X x	user	nicole_andy4	✓	18 hours ago	2026-04-07 20:31	Profile	Edit
X x	user	Neildiamond4041	✓	6 hours ago	2026-04-08 08:58	Profile	Edit
X x	user	MJTruethUltra	✓	never	2026-04-08 09:06	Profile	Edit

Fig. 5: The 21 Nigerian accounts whose followers and following were collected in this phase.

Handle	Name	Type
UrogdiG	Ürögdi Géza	Hungarian
PatriotXXsz	Imles 🇭🇺🇸🇦❤️+👍🇨🇭	Hungarian
SSzigyarto	Stefan Szigyarto 🇭🇺💙🇩🇪	Hungarian
sookymari	moompah	Hungarian
RNascal	Róbert Nádasy	Hungarian
mondolecske	Möndölecske Fekete 🇭🇺	Hungarian
Leslie1899x	Ladislaus	Hungarian
huxit2026	HUXIT2026	Hungarian
GborLukcs4	@GborLkcs4	Hungarian
70lili0508	Ariett 🇭🇺🇵🇷	Hungarian
zenkucko	Zenkucko.hu 🏠	Hungarian
SzakacsPisti82	Istvan Szakacs	Hungarian
nzsandras	csakazértis! ❤️🇭🇺😬	Hungarian
NmethTa1974	Németh Tamás 🇭🇺	Hungarian
kosFarag260673	Ákos Faragó	Hungarian
kunpisti	Kun István	Hungarian
JuditJanosne	Judit 🇭🇺	Hungarian
Jeszy661937	Jeszy	Hungarian
gondolat126906	gondolat	Hungarian
DetiBernadette	Deti 🇭🇺🇵🇷	Hungarian
BollerLeo	Balambér (Nem félek!)	Hungarian

Fig. 6: Hungarian accounts which are followed by the identified network.

Following the collection of follower and following data for the 21 Hungarian accounts listed in Fig. 6, Trollensics extracted location data for all associated accounts. Location data on X is returned across two fields: *Account Based In* and *Account Source*. *Account Based In* may return one of the following: a specific country, no location data, or a broad geographic region such as "Africa" or "East Asia." *Account Source* typically returns a country combined with a platform identifier, for example, "Hungary Android App" or a regional equivalent such as "Africa Android App." Where no location is returned, one of three conditions apply: the account has no associated country and its source is listed as web; the account is locked, in which case neither field returns any data; or the account has been suspended or deleted, again resulting in no data across both fields.

Analysis of the follower and following data for the 21 Hungarian accounts confirms that all Hungarian accounts are followed by bot accounts geolocated to Nigeria (1040 total followers). The total number of automated accounts geolocated in Asia and West Africa reached 1,770 total followers. The full breakdown of country specific insights can be found below in Fig. 7:

Location	Number of followers
Africa	222
Benin	31
Ivory Coast	28
Gambia	55
Ghana	59
Nigeria	1040
Cambodia	25
Hong Kong	79
Pakistan	56
Singapore	26
Thailand	27
Vietnam	98
West Asia	24
Total	1770

Fig. 7: The breakdown of followers with available geolocation data, following Hungarian accounts.

The CIB assets following Hungarian accounts can be categorised into several distinct types, exhibiting different signs of automation. The largest category, present overwhelmingly in the followers located in Nigeria, consisted of celebrity and public figure impersonation accounts. The dataset contains dozens of accounts impersonating Elon Musk, operating under usernames such as @elonmusk_x0150, @Ceo_Of_AllTesla, @CEOTESLA112399, @elonmuskspavex, and @c_e_o_T_musk26, among many others. Several accounts impersonate members of his family, including multiple variants of his mother Maye Musk (@maye9533, @MayeX_500, @mayeprivate2926, @officialmaye178, and at least a dozen more), his children Saxon Musk, Vivian Jenna Wilson, and Griffon Musk. Further impersonation targets include Donald Trump, Barron Trump, Ivanka Trump, Tiffany Trump, Jason Momoa, Robert Plant, Keith Richards, Brad Paisley, and

Matteo Bocelli. Many carry explicit disclaimers such as "parody account" or "fan page," while others present themselves as official or legitimate backup accounts.

A second distinct type of accounts was found mostly in the followers located in Vietnam, characterised by an almost uniform naming convention of generic Anglo-American first names paired with common English surnames and a numerical suffix, such as @AaliyahJoh90602, @AbigailJon3398, @HaileySmit77279, @GraceJones41143, @NatalieJon38348, and @ValentinaW43965. The pattern of numeric values at the end serves as a clear indicator of CIB account generation. Post counts are uniformly low and following counts are moderate, consistent with accounts created in bulk for amplification efforts rather than content production.

Another type of accounts is found in Hong Kong, where of 79 Hong Kong-geolocated accounts in the dataset, 20 share an identical biography: "Gods determine what you're going to be." including the distinctive Chinese-language full-stop character. They also have structural similarities with having zero recorded posts, all created between March 2025 and September 2025 with some created on the same day. These accounts also follow between 1,400 and 3,900 accounts despite having little to no following of their own. This also hints at this being a batch of accounts produced from a single template and deployed simultaneously.

Across all country clusters, a common behavioural sign is the high following counts relative to near-zero post counts. The pattern of accounts following several thousand other accounts while having posted once, never, or only a handful of times since observed vastly across this dataset. All of these markers together suggest that these assets were created not to produce content, but to manipulate platform recommendation algorithms. The Hungarian target accounts flagged by are the beneficiaries of this manipulation, accruing an artificially inflated appearance of reach and social credibility manufactured entirely from abroad.

Another particularly notable finding concerns the volume of accounts attributed to the United States displaying characteristics consistent with MAGA-affiliated profiles. All 21 Hungarian accounts are followed by large numbers of such accounts, and it is assessed that these are likely part of the broader Nigerian network operating under American-facing personas. The most striking individual case is the account *huxit2026*, which has 6,461 followers in total, of which 3,207 (approximately 50%) are American MAGA-style accounts, against only 744 followers identifiable as Hungarian. This

disproportion is a strong indicator of artificial inflation of the account's apparent reach and domestic support base.

Notably, the primary activity of these networks was not content amplification through retweeting. Instead, the defining behaviour was the mass following of pro-Orbán and pro-Russian Hungarian accounts. This pattern is significant in the [context of recommender system dynamics](#) - platforms such as X use follower graphs as input signals for content recommendations. When a large number of accounts (even inauthentic ones) follow a particular account or cluster of accounts, the recommender system may interpret this as a signal of relevance or popularity, artificially boosting the reach of that content to genuine users. This mechanism, sometimes associated with CIBs, represents a form of manipulation that operates below the threshold of direct content posting, making it harder to detect through conventional content-based analysis. Based on this theory, Trollrensics analyzed the accounts mainly responsible for using/retweeting the most used hashtags during the elections. These accounts were the same accounts that were followed by the CIB networks.

Data analysis

Data provided by Trollrensics has also been independently analysed by Alliance4Europe. With the shared insights on followers from the identified accounts stated previously in Fig. 8, we were able to analyse statistical insights on follower overlaps and geographic locations. Data analysis reveals that out of all unique followers across the 21 Hungarian accounts identified by Trollrensics, 16.8% of their audience appear to overlap (i.e. appear as followers of two or more accounts). The breakdown of basic statistics is available in Fig. 8 below, outlining the total number of followers, as well as basic values of overlapping followers.

Metric	Value
Total unique followers across all accounts	22,082
Followers appearing in 2+ accounts (overlapping)	3,701
Overlap rate (% of unique followers)	16.80%
Followers appearing in 10+ accounts	155

Followers appearing in 15+ accounts	41
-------------------------------------	----

Fig. 8: Follower overlap analysis across the 21 Hungarian CIB Accounts

We were also able to analyse the statistical distribution of overlap in followers across accounts. The table below in Fig. 8 assesses the amount of follower overlap per number of accounts followed, meaning how many accounts have been followed by a singular overlapping account. The majority of overlapping accounts have been following 2 accounts at one time; however, a significant number of overlapping accounts have followed 10+ CIB-designated accounts at one time. 30 followers appear across 10 or more of the 21 accounts simultaneously. The most extreme case is the account of @Pppimre, which follows 19 accounts in the dataset.

Appears in N Accounts	Number of Followers
2	1907
3	647
4	351
5	182
6	125
7	83
8	42
9	38
10	38
11	19
12	18
13	13
14	18
15	9
16	11
17	4
19	1

Fig. 9: Statistical distribution of overlapping followers per identified CIB account.

There has also been a notable per-account overlap, as some accounts share a striking overall overlap between each other. The highest rate of overlap is *JuditJanosne* with 86.3% of the account's followers overlapping with other accounts in the identified list of Hungarian accounts. The account *kosFarag260673* comes close with a 75.6% overlap, shortly followed by *BollerLeo* (70.0%), *sookymari* (69.9%), *DetiBernadette* (65.9%), *NmethTa1974* (65.9%), and *Leslie1899x* (62.4%). This data indicates that the majority of these assets' followers are shared with other accounts in the dataset, which supports the hypothesis of these accounts targeted by coordinated inauthentic behaviour networks.

Account	Total Followers	Overlapping Followers	Overlap %
UrogdiG	4485	1971	43.90%
DetiBernadette	2364	1559	65.90%
SzakacsPisti82	2782	1422	51.10%
RNascal	2638	1215	46.10%
huxit2026	6462	952	14.70%
BollerLeo	1266	886	70.00%
Jeszy661937	1635	878	53.70%
SSzigyarto	1892	572	30.20%
GborLukcs4	1447	565	39.00%
Leslie1899x	707	441	62.40%
JuditJanosne	511	441	86.30%
mondolecske	848	305	36.00%
sookymari	395	276	69.90%
PatriotXXsz	997	271	27.20%
kosFarag260673	291	220	75.60%
NmethTa1974	314	207	65.90%
nzsandras	391	197	50.40%

kunpisti	1283	196	15.30%
70lili0508	223	123	55.20%
gondolat126906	106	45	42.50%
zenkucko	127	41	32.30%

Fig. 10: Per-account follower overlap of Hungarian accounts based on data provided by Trollrensics.

Of 21,702 unique followers identified across the 21 Hungarian accounts, 3,506 appear as followers of two or more accounts simultaneously. While a degree of organic overlap is expected within any ideologically coherent community, the distribution of followers overlap together with the previous engagement of these assets in a potential influence operation linked to the Dutch elections raises concern. The pairwise overlap analysis reveals a core cluster of accounts that share very large numbers of followers with each other: *UrogdiG*, *RNascal*, *DettiBernadette*, *SzakacsPisti82*, and *Jeszy661937*. The pair *RNascal–UrogdiG* alone shares 887 followers; *DettiBernadette–UrogdiG* shares 835. Another interesting finding is once again a repeat of the Dutch modus operandi with accounts that have been created within a name cluster. Six variants of the name Azara/Yucil were found in the naming patterns across the dataset: *@AzaraYucil70847* (Nigeria, following 7 Hungarian accounts), *@azara_yucill* (Africa, following 5 accounts), *@AzaraYcil162292* (Nigeria, following 4 accounts), *@YucilAzara55966* (following 4 accounts), and others. All are geolocated to Nigeria or unspecified Africa, all have very low post counts (2–12), and all follow far more accounts than follow them. Broadly speaking, most of the accounts present with typical bot-like inauthentic naming conventions, inconsistent posting and following patterns.

Lastly, analysis was undertaken based on the provided data to understand the geographical locations of the overlapping accounts. Whilst that data is not always available in the scraped dataset, as per the earlier indication, the country most often appearing across the overlapping accounts was once again Nigeria. Nigeria scored highest by a large margin, with the second largest cluster of accounts operating from Vietnam. The full breakdown of countries listed in the accounts’ bio can be found in fig. 11 below.

Country	Overlapping Followers
Nigeria	104
Benin	16
Ghana	12
Viet Nam	32
Thailand	5
Hong Kong	3

Fig. 11: Available data on the operation country of origin for the CIB followers.

Conclusion

What makes this operation concerning is its strategic repeatability and the ease with which its assets can be repurposed across different political contexts. The behavioural patterns identified in the Dutch election dataset, such as mass following of small hyperactive accounts, selective amplification of far-right and anti-institutional content, the use of accounts that cycle through different identities while maintaining the same operational function, are strikingly consistent with those observed in the Hungarian dataset. In both cases, the same network of accounts, geolocated primarily to Nigeria and other West African countries, was found following and amplifying pro-Orbán and pro-Russian Hungarian language accounts. The accounts do not need to be rebuilt between operations, they require only a change of front-facing information such as profile, profile picture and bio. A fake account that retweeted Dutch election-related content in October 2025 can, and has, with minimal modification begun following and reposting Hungarian content in the wake of the upcoming elections. This interoperability is a defining feature of the operation, which also raises questions about potential X terms-of-service breaches and appropriate changes in regulation or enforcement.

The cumulative effect of this activity is the fabrication of an artificial information sphere. As exemplified by the repeated example in the Netherlands and now Hungary—what appears to be an organically growing ecosystem of localised accounts expressing far-right, pro-Russian sentiment is in reality a coordinated attempt at swaying voter behaviour. The difficulty of identifying those accounts with an untrained eye is concerning, as accounts with Hungarian-language content, Hungarian names and bio’s build an illusion of localised, authentic voices. As a result, posts promoting Eurosceptic, pro-Orbán, or anti-NATO content appear to gain traction online despite lacking genuine popular support due to amplification of polarising content by foreign CIB networks. The CIB

networks utilise known vulnerabilities in the systems platforms use to determine what content is pushed by the algorithm. The result is a distorted information environment in which ordinary users, journalists, and even policymakers may draw conclusions about the state of public opinion based on data that has been deliberately falsified.

This operation fits a well-documented pattern of interference that recurs around elections and major political events across Europe. The infrastructure does not disappear between election cycles, and as such, the Netherlands and Hungary are unlikely to be the only cases, should this behavior continue to remain permissible on the X platform. X, while suspending a portion of identified accounts, as far as we have been able to ascertain, has not addressed the underlying platform vulnerabilities that make this form of manipulation possible. Additionally, the platform has reduced researchers' ability to detect and document such operations by removing publicly visible engagement metrics such as likes on a post, which used to be a reliable method to conduct research in CIB networks and amplification operations. This change narrows the data and evidence available to investigators without in any way impeding the actors carrying out influence operations. The pattern of partial and reactive account suspensions, where the platform removes some nodes while leaving the broader network intact and active, raises questions about the effectiveness of platform moderation. Whilst X can claim to have taken action to suspend users implicated in an influence operation, too little is done to disrupt the operational capacity of the threat actor. Some accounts that appeared in both the Dutch and Hungarian datasets remain active despite being flagged as inauthentic. As long as these assets are allowed to operate, the same infrastructure can be pointed at any forthcoming election, in any country, at minimal cost and with minimal risk to those operating it, threatening the electoral processes across Europe.