FOREIGN INTELLIGENCE SERVICE

NOTE

Analysis of national security risks generated by the actions of state and non-state cyber actors on IT&C infrastructures, support for the electoral process

Unclassified extract from Note no. 0654 of November 28, 2024

- Russia has a history of interfering in the electoral processes in other states. If in the ex-Soviet space Russia was and is quasi-present through hostile actions of influence, in the West, the involvement has become much more evident starting with 2016/ the US presidential election.

Russia's interest in such hostile actions directed towards the West has increased in intensity, with an increasingly complex modus operandi, a very large share of the actions being carried out in the online environment, since: a) it is difficult to identify the connection between the operations themselves and individuals; b) Russian services were forced to adapt and made the transition from classic influence actions (managing human resources through traditional methods) to online actions.

- This year, several elections took place in the West, including the European Parliament elections/June 2024, with Russia conducting, to varying degrees, influence actions. The following preliminary conclusions regarding Russian interference emerged:

- by order of Kremlin, detailed sociological research was conducted on the target states (trends in public opinion, political perspectives of certain parties/candidates, measures taken by the authorities against foreign electoral interference) and what is the response capacity;
- informational aggression, including propaganda, and the use of artificial intelligence for rapid content creation were emphasized;

In the Western online space, Russia has made constant efforts to access the widest possible audience categories, by expanding the online infrastructure (varied portfolio of dissemination channels, official vectors, local trainers and troll networks) and diversifying the techniques for spreading (pro)Russian narratives, with an emphasis on their distribution at the local level (e.g. coordination of messages, increasing the quantity and quality of multimedia content, including using : artificial intelligence/AI software; hijacking and creation of hashtags, mainly on the X network);

- Moscow's interest in increasing the chances of pro-Russian, far-right, anti-system candidates, "pacifists" and representatives of nationalist movements is maintained. In the Kremlin's view, the European far-right is receptive to Moscow and is on an upward trend in popularity.

Russia has flooded the information space with divisive narratives and in support of vectors (persons or political formations) with views close to the Kremlin (extremists, nationalists, populists, anti-system political figures, etc.).

Tactics, techniques and procedures: creation and consolidation of extensive networks of online platforms and channels/groups on social media, development of support/pro-Kremlin networks, which will subsequently act as vectors for promoting Russian narratives, with an emphasis on local opinion leaders with Eurosceptic visibility/visions; diversification of methods to circumvent Western measures; organization of cultural events dedicated to Russian values/policies; taking statements by European officials out of context; fueling conspiracy theories; creating deepfake content to defame inconvenient candidates.

The scheme of dissemination/amplification of messages remained decentralized: local pro-Russian satellites, clones of famous websites, accounts/channels and troll networks on social media platforms;

Objectives: amplifying the population's fears regarding the deterioration of the security situation; undermining trust in authority by discrediting European leaders, officials/ruling parties and victimizing the opposition (the "totalitarian Europe" thesis); highlighting the negative impact of their policies/decisions on the socio-economic situation; strengthening the position of Eurosceptic and extremist leaders/formations; eroding political and social support for Ukraine; amplifying social discontent;

- **capitalizing on the passivity** of the authorities to create gaps in public opinion.

■ during elections organized in the Republic of Moldova, techniques of adapting information manipulation according to demographic groups (e.g. nationalists, religious communities, rural population, vulnerable citizens) were noted, with the help of viral videos and emotionally charged images used to provoke strong negative reactions. The narratives are alternated according to 'political developments, ensuring their relevance, and the messages transmitted on Telegram, Facebook, lnstagram, TikTok and VKontakte are coordinated and uniform.

• Romania is perceived by decision-making centers in Moscow as an enemy state (,,unfriendly"), and according to our data, Moscow adopts a policy of active deterrence towards Romania.

In Russia's view, our country:

- "provokes and threatens" Russia's security through the NATO and American military potential it hosts;
- "wants to solve its economic problems at the expense of Russia" (the Treasury issue);
- represents a direct competitor in the Republic of Moldova.

Romania - along with other states on NATO's Eastern Flank - has become a priority for Russia's hostile actions, with the Kremlin having a growing interest in influencing (at least) the MOOCL and the agenda in Romanian society in an electoral context through:

- propaganda and disinformation (including by using emerging technologies in activities targeted at specific groups and communities - e.g. by aggregating publicly available data - e.g. political, economic and media consumption preferences - and implementing generative artificial intelligence modules through which they can transmit adapted propaganda messages, in real time'. at the individual level};
- supporting Eurosceptic candidates and fueling anti-system movements, including by

"Involving them in protests to shape the public agenda;

- encouraging discontent/provoking emotional reactions at the level of population, to put pressure on the authorities to reduce/stop support for Ukraine.

We appreciate that Romania is a target for Russian aggressive hybrid actions, including cyber-attacks and information leaks (hacks'and leaks) and sabotage.

It must be noted that during this year, the political situation in Romania was also addressed in political talk shows in Russia - Russian journalists are launching the idea that pro-Russian forces in Romania could obtain over 30% in the parliamentary elections. '

• The analysis of the way in which the Russian propaganda apparatus targeted Romania in 2024 highlights an approach:

- indirect, through the membership in NATO and in connection with the support granted to Ukraine and the Republic of Moldova, references being triggered by developments on these issues/spaces;
- directly, through information operations in the context of the increase in "Romania's threats to Russia's security" in the form of expansion on the Eastern flank, in the violation of national airspace by Russian

drones and disinformation about the burning of warehouses on the national territory by so-called Ukrainian refugees.

The messages aimed to: (i) divide society on issues such as the control exercised by the US/NATO over Romania, the security threats generated by NATO membership and support for Kiev; (ii) discredit NATO and Romania's response capacity, amplifying the population's distrust in the national defense capacity; (iii) erode the population's support for Romania's foreign policy decisions; (iv) highlight Romania's involvement in the conflict and territorial ambitions in relation to neighboring states (e.g. Ukraine and the Republic of Moldova).

In the case of information operations that directly targeted Romania, the modus operandi was similar to other propaganda actions launched in the European space since the beginning of the war in Ukraine: the same strategy of creating and validating fake news (through multimedia content and extensive false details), the use of similar methods of promoting and circulating the content (same initial source; same accounts involved in promoting the message; same audiences) and the erroneous connection of events with Ukrainian vectors (refugees or the resistance movement).

Tactics, Techniques and Procedures:

i) the use of photo-video materials whose veracity is difficult to prove - recordings of the alleged incidents (do not contain visible elements of identification, the initial source or location of the filming cannot be identified), accompanied by exaggerations regarding their magnitude; photos taken from older articles in the local press and manipulated (e.g. cropping the date of an image regarding a fire from July 31, 2024 in Bragadiru);

ii) mass rolling (cross-posting) through approximately the same accounts, on multiple social networks (X, Telegram, Facebook):. were engaged: Russian propaganda vectors aimed at the Russian public, including political analysts/ scientists or church-associated accounts, (pro)Russian accounts dedicated to covering the war in Ukraine and accounts with high visibility in the European space
(e.g. audiences in English, French, German, Turkish/Spanish), but also among the Arab and Chinese audience.

Such informational actions give credibility to subsequent news regarding sabotage incidents (true or false), generate panic and distrust in authorities and manipulate the collective mind (especially the audience with a low level of media culture) to place responsibility on the Ukrainian vector from the start.