Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Is Europe immune to Chinese interference in its electoral processes?

While Europe has been focused in recent years on defence against Russian cyber interference in its political life, it seems to ignore the danger of China following the same path at some point.

Why shouldn't the European Parliament elections in June and a series of national elections across Europe this year serve as a decisive live test of China's cyber systems, this time directly regarding political events?

China's malignant activities in cyberspace have traditionally focused on industrial espionage, in large part on controlling and influencing its large diaspora in Europe, particularly dissidents, their environment, and their activities, so that they could suppress them in time or reduce their harmful influence on the regime in Beijing.

However, numerous reports and assessments agree that China has essentially abandoned its defensive mode in the cybersphere, and particularly its lack of interest in political influence in Europe.

Alarms from Lithuania and France

Lithuania will hold presidential elections in May, elect 11 members of the European Parliament in June, and hold national parliamentary elections in October.

In early March, the government's security services issued worrying assessments that this series of elections could be vulnerable to attacks on the electoral process by Chinese cyber actors.

“The scenario of attempting to influence elections definitely cannot be ruled out. I am mostly referring to China”, said Darius Jauniskis, then head of the Lithuanian State Security Department.

> Lithuania has reasons to expect Chinese attacks and an attempt to influence the election process

The Baltic state has reasons to expect Chinese attacks and an attempt to influence the election process because it has been leading the way with a harsh policy towards Beijing within the EU.

First of all, because of its affection and support for Taiwan, but also because it was the first EU member to leave the cooperation programme of Central and Eastern European countries within the Chinese Belt and Road project.

The French Parliament concluded earlier that increasingly aggressive attacks aimed at political objectives should be expected from China, including information manipulation, cyber-attacks, spreading fake news and narratives, and espionage.

Last year's parliamentary report, prepared for months at the request of Marine Le Pen’s ultra-right National Rally, warned that China had been following Russia's footsteps regarding methods of malignant influence on political processes in France.

The head of the French External Intelligence (DGSE), Bernard Emié, said that China had gone from a "contained power" to an "aggressive power," primarily with the help of its "unbridled diplomacy."

Warning from the UK

The European Parliament has warned all members of the Union that foreign interference through disinformation and attacks on democratic institutions will be even more frequent and sophisticated ahead of the elections in June.

China, along with Russia, has been identified as a source of this type of influence, not only in EU member states but also in candidate countries, such as the Balkans, and countries of the so-called Global South.

The recent discovery that state-sponsored Chinese companies hacked the data of 40 million voters in the UK for a full 14 months from 2021 to 2022 sets a good example for the

EU regarding where it could expect typical Chinese interference in electoral and political processes.

Hacking the lists of the UK's Electoral Commission is a model that China will apply to the EU members as well, given that significant elections are coming up in both countries, followed by campaigns in which the stakes will be high.

Some EU countries may already be victims of such attacks by Chinese cyber groups if we keep in mind that the British case was confirmed only a year after it happened.

> The mere recognition that the electoral infrastructure is compromised causes the public to lose confidence in the electoral process

But the goal is the same. The mere recognition that the electoral infrastructure is compromised causes the public to lose confidence in the electoral process and in the democratic institutions that implement it, including the politicians and parties that participate in it.

Ultimately, the objective is for voters to be sceptical about the officially stated election results.

Chinese interference and the growth of the European right

This strategy of destroying trust in democratic institutions is well known from the 2020 US presidential elections, which ultimately led to Donald Trump's attempt to stay in power by force and his supporters invading the US Congress in January 2021.

The consequences are strong even today when Trump rushes towards a new presidential candidacy with the significant support of Republican voters, who are still convinced that the 2020 elections were stolen.

European populists could easily embrace the idea that the elections have been manipulated by the European establishment

China might be interested in the same goal in the European Union this year, given that anti-establishment, Eurosceptic, and ultra-right forces are expected to increase in June's European Parliament elections as well as in a series of national elections.

As in the US almost 4 years ago, European populists could easily embrace the idea that the elections have been manipulated by the European establishment and perhaps start more serious protests and destabilise European political life.

For that, it is necessary to first reduce trust in institutions, compromise some parties and their leaders, and publish fake narratives and misinformation.

All this could be provided by state-controlled hacker entities launching attacks and intrusions into the databases of European electoral institutions, political parties, parliaments, and government agencies. Clearly, they have already started.