European Election Security At Risk: A Detailed Analysis of State-Sponsored, eCrime, and Hacktivist Threats

quointelligence.eu/2024/06/european-election-at-risk-analysis/

June 5, 2024

As the European Elections approach, concerns about election integrity intensify within an ever-evolving and increasingly polarized threat landscape.

This blog post will provide a detailed exploration of the diverse and complex threats facing these pivotal elections. Through expert analysis, we aim to unravel the multifaceted nature of these cyber threats, enhancing understanding and preparedness among stakeholders.

BLOG
EUROPEAN ELECTION SECURITY AT RISK
A DETAILED ANALYSIS OF STATE-SPONSORED, ECRIME, AND HACKTIVIST THREATS
QUOINTELLIGENCE

QuoIntelligence's analysis shows that state-sponsored operations are the main threats to European election security, with political entities and media as primary targets.

- Russian state-sponsored activity is the most likely to affect election security, with a high likelihood of cyberattacks and hybrid warfare operations involving physical and cyber aspects.
- Political figures and parties, government entities, and media platforms are most likely to be targeted by such operations.
- Ransomware and supply chain attacks can alter the smooth running of the elections but do not threaten their outcome.

- Financially motivated threat actors are unlikely to intentionally disrupt the electoral process.
- Pro-Russia hacktivist groups will likely launch short-lived DDoS attacks targeting European entities amid the elections, causing limited impact.

State-backed activity poses HIGH RISK to the EU Parliamentary election security (high likelihood, medium impact)

Russian and Chinese state-sponsored threat actors are the foreign actors most likely to interfere in the EU's parliamentary elections in June.

Russian State-sponsored Activity Will Highly Likely Attempt To Disrupt European Parliamentary Elections. Since the beginning of the Russian invasion of Ukraine in February 2022, tensions between the EU and Moscow have grown significantly. On the threat landscape, this materializes through the intensification of Russian hybrid warfare operations. Notably, since April, the North Atlantic Alliance and other European security services have publicly warned of Russian information and espionage operations, as well as physical sabotage.

High Risk of Cyberattacks: In May, Germany denounced cyberattacks conducted by **APT28** against the Social Democratic Party (SPD).[1] More, recently, the Polish government reported that the country's state news agency's website was the target of a cyberattack which resulted in the publication of a false story about military mobilization to fight in Ukraine. The authorities suspect this to be a Russian state-sponsored attack to destabilize the EU ahead of the European Parliamentary elections. Further cyberattacks are likely ahead and after the European elections. They can serve several purposes: disruption, influence, and espionage.

Among Russian APTs, we assess that **APT28** and **APT44** (aka Sandworm), both affiliated with the Russian General Staff Main Intelligence Directorate (GRU), are most likely to take part in cyber operations aiming to disrupt the elections as they have engaged in similar campaigns by the past. Notably, **APT28** was involved in attempts to influence the US presidential election in 2016 and the French presidential election in 2017.

High Risk of Hybrid Influence Operations: Over the last months, Russia has intensified its efforts to sow division in the EU through covert hybrid influence operations. French intelligence service reportedly identified the FSB Fifth Service behind the tagging of stars of David in the streets of Paris in November 2023. This operation was then amplified by an online campaign that involved thousands of bots linked to the infrastructure of the Russian widespread disinformation campaign, Doppelganger, publishing content about the controversy on X. Similar operations are highly likely in the short term. In fact, another incident is pointing to continuous efforts of Russian services to sow division. On 1 June, three individuals staged five coffins draped in a French flag and bearing the inscription

"French soldiers of Ukraine" near the Eiffel Tower. Police have arrested the individuals involved in this incident and authorities have reportedly established some connection between this incident and the Star of David case.[2]

High Risk of Espionage Operations: Russia is conducting long-term espionage operations in Europe, using both traditional means of recruiting agents, including within the European Parliament,[4] and cyber operations. Russian services will likely monitor the electoral process and identify new targets among the new Members of the European Parliament (MEP) and staff.

Chinese State-sponsored Espionage Activity Highly Likely Amid European Parliamentary Elections

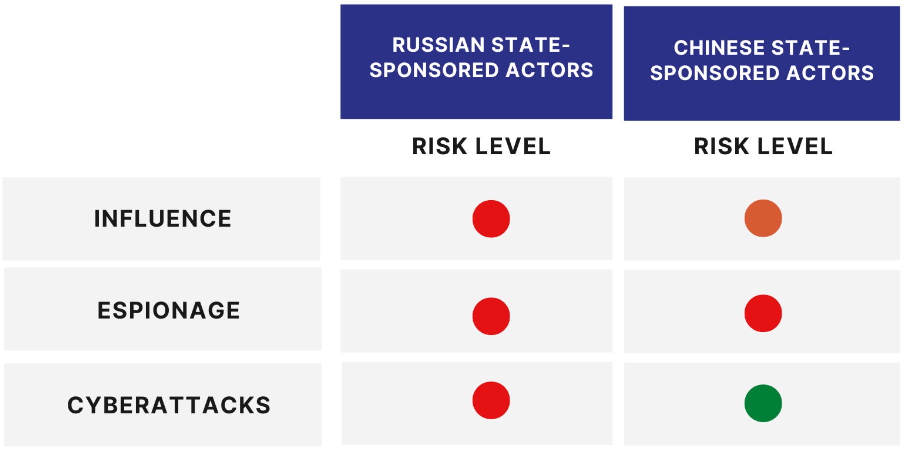
Throughout 2024, the EU has taken measures aligned with its new policy to de-risk trade with China, contributing to tense its relations with Beijing. Coupled with the growing polarization of the global geopolitical landscape, this increases the probability of some sort of Chinese interference in the EU's parliamentary elections. We assess that direct cyberattacks conducted by Chinese state-sponsored threat actors are unlikely, while influence operations are more probable.

High Risk of Espionage Operations: Recently, espionage cases in the European Parliament[5] and in the UK[6], have illustrated the scale of Chinese espionage in European political institutions. Beijing will highly likely continue to engage in such activities before, during, and after the European elections to anticipate the outcome and then adapt its strategy accordingly. The groups linked to China's Ministry of State Security (MSS) are most likely to engage in such activities during the European elections. The MSS conducts intelligence collection using human intelligence and cyber operations. The **Winnti Group**, which includes **APT17**, **APT41**, and **APT15**, is known for state-sponsored espionage operations targeting entities in Europe, Asia, and North and South America, with victims in governmental institutions and other strategic sectors. In 2023, researchers identified a Chinese espionage campaign conducted by **APT15** which ran for months targeting foreign ministries.[7] More recently, in March, the US and the UK denounced espionage operations conducted by **APT31** targeting high-ranking government officials and their advisers.[8]

Medium Risk of Influence Operations: In 2024, reports have already identified Chinese threat actors behind influence operations in the framework of elections. In fact, the Taiwan presidential election, held on 13 January, illustrated the widespread use of artificial intelligence-generated content as part of an influence campaign that was likely orchestrated by Chinese actors. Notably, we observed the spreading of visual and audio deepfakes of pro-independence candidates and public figures, aiming to discredit the pro-independence party, the Democratic Progressive Party (DPP). Other TTPs used during this campaign included fake opinion polls, fake news websites, AI-generated news anchors, and AI-generated memes. Our analysis has shown that AI-powered influence operations have not been effective in changing the outcomes of an election. However, threat actors are likely to continue to experiment with the use of AI, exploiting rumors, bias, defamatory content, or controversial political questions to develop online disinformation campaigns.

We assess that Chinese state-sponsored threat actor **Storm-1376** (aka Spamouflage and Dragonbridge) is most likely to engage in such activity. In fact, the group was identified behind multiple information operations including the discrediting of pro-democracy protests in Hong Kong in 2019,[9] attempts to mobilize protesters in the US in the context of the Covid-19 crisis,[10] and efforts to discourage Americans from voting in the 2022 US midterm elections.[11]More recently, Microsoft reported in April the involvement of Storm-1376 in multiple influence operations targeting Taiwan, the US, Japan, and South Korea.[12]

RISK LEVEL OF RUSSIAN AND CHINESE STATE-SPONSORED OPERATIONS FOR THE EUROPEAN ELECTIONS



	RUSSIAN STATE-SPONSORED ACTORS	CHINESE STATE-SPONSORED ACTORS
	RISK LEVEL	RISK LEVEL
INFLUENCE	🔴	🟠
ESPIONAGE	🔴	🔴
CYBERATTACKS	🔴	🟢

This table describes the risk level of the different types of Russian and Chinese state-sponsored operations

🔴 HIGH 🟠 MEDIUM 🟢 LOW

Political Figures and Parties, Government Entities, and News Outlets Most Likely To Be Targeted

Political figures, assistants, and political parties are exposed to:

- Smear and disinformation campaigns aiming to degrade them.
- Data leaks exposing private communications, strategies, and other confidential information, potentially altering public perception and political outcomes.
- Espionage for data collection and possible posterior recruitment effort.

Governmental institutions are exposed to:

- Espionage: Governmental institutions remain prime targets for cyber espionage. Threat actors seek to collect sensitive data that could be used to gain strategic advantages or influence governmental operations.
- Sabotage: There is a persistent threat of disruption attempts against governmental operations. This includes cyberattacks designed to disable infrastructure, spread confusion, and hinder governmental functions.

The media sector is exposed to:

Discrediting legitimate sources: Media outlets can be targeted to undermine their credibility, thereby eroding public trust, sawing confusion, and making it easier to propagate alternative or false narratives.

eCrime activity poses MEDIUM RISK to the EU Parliamentary election security (medium likelihood, medium impact)

Ransomware and supply chain attacks affecting IT providers of the election infrastructure are the most likely financially motivated cyberattacks that election security may face.
Elections in almost all EU countries are conducted using paper ballots. As such, influencing the outcome through cyber means is unlikely. However, an attack can:

- Disrupt voter registration,
- Render unavailable poll books,
- Thwart adjacent IT infrastructure used to communicate instruction to the voters or coordinate government efforts and operations,
- Impact the transmission of results from polling stations and therefore delay the communication of results at the national level.

Some of these scenarios would contribute to eroding the voters' trust in the electoral process and could even discourage citizens from voting.

In October and November 2023, a ransomware attack affected 103 German municipalities after the breach of the local municipal service provider Südwestfalen-IT. Multiple servers were offline for at least 17 days after the attack. Analysis of the infrastructure of Südwestfalen-IT reveals that it is used for hosting election-related services on behalf of the government administration. A similar attack ahead or during the electoral process could disrupt services related to election organization systems, thereby affecting election security.
We assess that eCrime actors are unlikely to willingly target election infrastructure and their IT providers during the EU parliamentary election. While monetary gain could be significant, there is little incentive to disrupt elections. In fact, such attacks would attract the attention of Law Enforcement Agencies (LEA), likely triggering threat disruptions operations.
Nevertheless, unintended disruptions cannot be ruled out due to the proliferation of ransomware and supply chain attacks.

Hacktivism poses MEDIUM RISK to the EU Parliamentary election security (high likelihood, low impact)

Pro-Russia hacktivist groups will highly likely continue to target European entities before, during, and after the European parliamentary elections. Their activity will highly likely take the form of short-lived Distributed Denial of Service (DDoS) attacks on layer 4 and layer 7 to cause resource exhaustion and system failure. Such attacks, easily mitigated with anti-DDoS solutions, are unlikely to disrupt election security. Less popular forms of attacks among pro-Russia hacktivist groups include web defacement, data leak, doxing, and social media hijacking.
Some pro-Russia hacktivist groups will possibly collaborate with **APT44** (aka Sandworm). In

April, Mandiant unveiled that **XakNet Team**, **CyberArmyofRussia_Reborn**, and **Solntsepek** are linked to **APT44**. As such, these groups could contribute to larger state-sponsored hybrid warfare operations.[13]

We assess that other forms of hacktivism are unlikely but cannot be totally ruled out. Radical groups could resort to some sort of cyberattacks as a means to amplify their messages and influence public opinion amid the electoral period.

1. Federal Ministry of Interior and Community, A2, 3 May, Cyber attacks traced to Russian military intelligence agency
2. Le Monde, B2, 3 June, Coffins at the Eiffel Tower: Suspicions point to another case of Russian interference
3. Politico, B2, 10 April, EU Parliament fines MEP accused of spying for Russia
4. Euronews, B2, 16 May, RussiaGate: German police search premises of leading far-right politician
5. Generalbundesanwältin beim Bundesgerichtshof, A1, 23 April, Arrested for suspected secret service agent activity
6. Financial Times, B2, 22 April, Former UK parliamentary aide charged with spying for China
7. Symantec, B2, 21 June 2023, Graphican: Flea Uses New Backdoor in Attacks Targeting Foreign Ministries
8. US Department of the Treasury, A2, 25 March, Treasury Sanctions China-Linked Hackers […]
9. Graphika, B2, 25 September 2019, Spamouflage – Cross-Platform Spam Network Targeted Hong Kong Protests
10. Mandiant, B2, 7 September 2021, Pro-PRC Influence Campaign Expands to Dozens of Social Media Platforms […]
11. Mandiant, B2, 26 October 2022, Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs […]
12. Microsoft, B2, 4 April, Same targets, new playbooks: East Asia threat actors […]
13. Mandiant, B2, 17 April, Unearthing APT44: Russia’s Notorious Cyber Sabotage Unit Sandworm

Research by Alixia Clarisse Rutayisire, Geopolitical Cyber Threat Intelligence Analyst at QuoIntelligence.

Alixia is an accomplished Geopolitical Analyst with extensive experience in cybersecurity and international relations. Prior to joining QuoIntelligence, she served as a Geopolitical Analyst for West Africa at the Ministère des Armées in France where she was responsible for analyzing geopolitical risks, including political and security situations, as well as internal and international conflicts.