July 2025
Deputy Chair ECe
Leiden Model United Nations 2025

Foreign Interference in National and European Elections

European Council for European Affairs (Ece)

Table of Contents

Table of Contents 1
Introduction 2
Definition of key terms 3
Algorithmic amplification 3
Artificial intelligence-generated content 3
Bot network 3
Cyberattack 3
Cybersecurity 3
Disinformation 3
Election integrity 3
Foreign election interference 3
Hybrid threat 3
Illegal political financing 3
Information warfare 4
Media literacy 4
Social engineering 4
State-sponsored interference 4
General Overview 5
Major parties involved 5
China 6
European Union 6
Russia 6
United States 7
Timeline of events 8
Possible solutions 9
1. Creation of a binding international framework for detecting and punishing foreign interference 8
2. Strengthening transparency and accountability in political advertising on the internet 8
3. Introduction of mandatory cybersecurity standards for national and EU election infrastructure 8

Introduction

In recent years, the threat of foreign interference in elections has become one of the most pressing challenges to democratic governance worldwide.
National and European elections are increasingly becoming the target of external actors seeking to manipulate political outcomes, destabilise societies and undermine trust in democratic institutions. This interference takes many forms, leading from cyber attacks on electoral infrastructure and the spread of disinformation via social media to covert financing of political parties and the use of diplomatic or economic pressure to influence domestic politics.

Foreign interference undermines not only the sovereignty of individual nations, but also the integrity of the democratic process itself.
Elections are the cornerstone of any functioning democracy.
When external powers attempt to influence voters or disrupt fair electoral processes, the legitimacy of elected governments is called into question. This is particularly worrying in the European context, where elections take place at both national and supranational levels and where interconnections between Member States can amplify the impact of interference from outside the Union.

A series of high-profile cases over the past decade has highlighted the scale and sophistication of these threats.
The 2016 presidential election in the United States, the Brexit referendum in the United Kingdom and the 2017 presidential election in France saw credible allegations of foreign disinformation campaigns and cyber operations, often linked to Russian actors.
More recently, EU institutions and national governments have expressed concerns about attempts by China, Iran and other states to subtly influence public opinion or gain strategic advantages through election manipulation.

Addressing this problem requires coordinated international action, improved cybersecurity, regulation of online platforms, and greater awareness among citizens and policymakers.
If left unchecked, foreign interference in elections could undermine democratic norms, strengthen authoritarian regimes, and lead to long-term geopolitical instability.
It is therefore not only necessary but also urgent to find effective multilateral solutions to this problem.

Definition of key terms

Algorithmic amplification

The process in which digital algorithms increase the visibility of certain content, which is often in favor of polarizing or sensational content, which can unintentionally lead to the spread of disinformation.

Artificial intelligence-generated content

Material such as text, images, or videos created with AI tools that can be used to mimic political figures, fabricate events, or manipulate public discourse during elections.

Bot network

A coordinated group of automated online accounts that are designed to simulate real users and spread or boost political messages, often as a part of foreign influence campaigns.

Cyber interference

The use of cyber capabilities to disrupt or manipulate information systems that are part of the election infrastructure, including voter databases, electronic ballots, and political party communication networks.

Cyberattack

An evil attempt to disrupt, damage, or gain unauthorized access to computer systems, networks, or data. This is often used to attack election infrastructure or political campaigns.

Cybersecurity

The practice of protecting systems, networks, and programs from digital attacks, particularly those which are aimed at accessing, altering, or destroying sensitive election-related information.

Disinformation

Intentionally false or misleading information created and spread with the intention of deceiving the public and manipulating political opinion.

Election integrity

The overall trustworthiness and fairness of an election process, including transparency, security, freedom from coercion, and protection from outside interference.

Foreign election interference

Deliberate efforts by foreign actors, either state or non-state, to influence the outcome, legitimacy, or public perception of an election in another country.

Hybrid threat

A combination of military and non-military tactics, including cyberattacks, disinformation and political interference, used by state or non-state actors to destabilize a country.

Illegal political financing

Unannounced or illegal financial support, often from foreign sources, used in violation of national laws to influence political campaigns, parties, or referendums.

Information warfare

The strategic use of information, including false or misleading content, to disrupt decision-making processes, weaken political institutions, and influence public opinion.

Media literacy

The ability to critically rate media sources, recognize bias or manipulation, and respond thoughtfully to political content, which is an essential skill for countering disinformation.

Social engineering

Psychological manipulation techniques used to trick people into revealing sensitive information or granting system access, often used in cyberattacks related to elections.

State-sponsored interference

Government actions that directly or indirectly aim to influence another country's electoral process, including through funding, cyberattacks, or information manipulation.

General Overview

Foreign interference in elections is a complex and constantly evolving challenge which threatens the foundations of democratic systems all over the world.
While the idea of foreign influence on domestic politics is nothing new, recent technological developments, especially the rise of social media, advanced cyber capabilities, and artificial intelligence, have strengthened the scale, speed, and the impact of these actions.
Foreign interference nowadays takes place through a wide range of means, often at the same time and involves both state and non-state actors pursuing political, strategic, or ideological goals.

The most well-known methods of interference include cyberattacks, disinformation campaigns, illegal political financing, and support for fringe political actors.
Cyberattacks can target voter registration systems, election counting software, party databases, or even politicians' private communication networks.
These attacks may aim to disturb the electoral process, publish sensitive data, or undermine confidence in the election results.
Disinformation campaigns involve the distribution of false or misleading content aimed at misinforming the public, sowing divisions, or discrediting certain candidates or institutions.
These campaigns are often carried out via coordinated networks of fake accounts and bots on social media platforms, with content tailored to exploit social tensions.

A common tactic is to promote extreme or divisive political narratives that polarize societies and weaken democratic agreement.
This not only influences voting behavior, but also damages long-term trust in democratic governance.
In Europe, foreign interference has often supported nationalist, Eurosceptic, or anti-immigration parties that challenge the stability of the European Union and its values.
In addition, foreign actors can exploit existing social divisions, like immigration, economic inequality, or cultural identity, to fuel disbelief and weaken national unity.

A key element of election interference is its covert nature.
Many operations are designed to be deniable, with attribution to specific actors often difficult or controversial.
This complicates international responses, as evidence may be insufficient to justify revengeful measures or sanctions.
Furthermore, some activities, such as the dissemination of disinformation or the financing of political organizations, may fall into legal gray areas, making regulatory action difficult.

The European Union has taken several measures to counter these threats.
The establishment of the East StratCom Task Force in 2015 was an important step in combating disinformation, particularly from Russian sources.
More recently, the European Action Plan for Democracy and the Digital Services Act aim to improve transparency in online political communication and hold platforms accountable for harmful content.
Nevertheless, differences in national cybersecurity capacities, regulatory approaches, and political will among member states disable a unified response.

The threat of foreign interference is also becoming increasingly transnational.
Disinformation can cross borders instantly, while cyber vulnerabilities in one state can threaten the security of the entire European electoral space.

Therefore, coordinated action between EU member states and with international partners is essential. In addition, civil society, the private sector, and media institutions must also be involved in efforts to protect democratic integrity.

Ultimately, foreign interference in elections is a form of asymmetric warfare in which external actors exploit openness and technological vulnerabilities to destabilize societies from within.
Without effective countermeasures, this phenomenon will further undermine public confidence in democracy and threaten long-term geopolitical stability.

Major parties involved

China

The People's Republic of China is increasingly involved in election interference operations, particularly in Europe and Africa.

While China's approach is less overtly disruptive than Russia's, it focuses on using economic leverage, diplomacy, and state-sponsored media to shape narratives that serve Chinese interests.

Chinese or Chinese-influenced platforms spread pro-Chinese messages, and there are growing concerns about the use of technologies such as TikTok and Huawei for data collection or influencing public opinion.

China's interest in influencing elections is generally consistent with long-term strategic goals, such as expanding its global influence, deflecting criticism of its domestic policies (e.g., human rights issues), and promoting divisions within Western alliances.

European Union

The European Union has recognized the growing threat of foreign interference in its democratic processes.

In response, it has launched several initiatives, including the European Democracy Action Plan, the Rapid Alert System for detecting disinformation, and partnerships with technology companies to increase transparency in political advertising.

The EU wants to promote media literacy, harmonize cybersecurity standards, and support member states in responding to hybrid threats.

However, the Union has limited ability to enforce measures, and much of the responsibility lies with national governments, leading to inconsistent implementation.

Russia

The Russian Federation remains the most active and aggressive state actor in foreign election interference.

Russia has developed a doctrine of information warfare in which influencing elections is an important tool for destabilizing rivals, particularly in NATO and the EU.

Through the GRU and other intelligence services, Russia has conducted cyber operations against election infrastructure and launched disinformation campaigns via platforms such as RT and Sputnik.

These operations often support systemically critical or extremist parties, promote voter apathy, or reinforce existing social divisions.

Russia denies involvement in such actions but has been sanctioned by several countries and institutions.

United States

The United States is both a key target and a strategic player in the global debate on election interference.

After experiencing significant foreign interference in the 2016 and 2020 elections, mainly from Russia, China, and Iran, the United States have strengthened its cybersecurity capabilities and promoted international cooperation on this issue.

Agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Homeland Security have developed programs to protect elections. At the international level, the US is working with allies through NATO, the G7, and bilateral channels to identify and prevent foreign influence.

Timeline of events

2014 May 25th	Russian-linked disinformation targets the European Parliamentary elections, particularly in Eastern European countries, promoting anti-EU and nationalist rhetoric.
2016 June 23rd	The Brexit referendum is heavily influenced by foreign-linked social media campaigns. Investigations reveal the presence of bots and coordinated misinformation promoting the “Leave” vote.
2017 May 5th	A major data breach in the French presidential campaign leads to the leaking of emails from Emmanuel Macron’s team. The incident is attributed to Russian group APT28, aiming to disrupt the election .
2018 November 6th	U.S. midterm elections take place amid heightened alert over foreign interference. The FBI and social media platforms coordinate in real time to remove disinformation accounts.
2019 March 19th	The European Parliament establishes a Special Committee on Foreign Interference to investigate past incidents and recommend protective measures for future elections..
2020 December 10th	The EU sanctions individuals from Russia, China and North Korea for their roles in attempted electoral interference and cyberattacks on EU institutions.
2022 April 6th	German intelligence reports evidence of Russian-backed cyber campaigns aimed at influencing the federal elections and public sentiment around the Ukraine conflict.
2024 September 1st	Elon Musk shares controversial posts on X supporting far-right narratives ahead of German state elections.German authorities warn of increasing foreign influence on voter sentiment via global social media platforms.

Possible solutions

1. Creation of a binding international framework for detecting and punishing foreign interference

Currently, there is no legally binding international mechanism that explicitly defines and criminalizes foreign interference in democratic elections. The creation of a United Nations-led convention or resolution could provide the necessary legal basis to define what constitutes election interference, including cyberattacks, disinformation campaigns, and illegal financing, and to create enforceable obligations for states.

Such a framework could require countries to establish national reporting mechanisms and submit regular transparency reports on foreign influence in their political systems. In the event of violations, signatory states could agree on sanctions or coordinated diplomatic measures. A global observatory on election interference could be established to collect evidence, support national investigations, and coordinate information sharing among democracies.
This solution would ensure long-term international commitment and lend legal legitimacy to countermeasures taken against the states concerned.

2. Strengthening transparency and accountability in political advertising on the internet

Much of foreign interference takes the form of digital manipulation of public opinion.
Foreign actors exploit the opacity of online platforms to spread targeted political advertising and disinformation, often without clear attribution or traceable sources of funding.
One of the most effective countermeasures is to introduce strict legal requirements for online platforms to clearly label political advertising, disclose who paid for it, and maintain publicly accessible advertising archives.

In addition, governments should require platforms to label automated accounts (bots), prohibit foreign companies from purchasing political advertising, and apply the same transparency rules across borders within regions such as the European Union.
These measures can be supported by independent election commissions, civil society watchdogs, and fact-checking alliances.
This solution directly targets one of the most effective and least regulated areas of modern interference, while preserving freedom of expression and political diversity.

3. Introduction of mandatory cybersecurity standards for national and EU election infrastructure

As cyberattacks on electoral systems become more frequent and sophisticated, there is an urgent need to introduce mandatory cybersecurity protocols for all components of the electoral infrastructure, including voting machines, vote-counting software, party communication systems, and voter databases.
In particular, the European Union should adopt a uniform cybersecurity framework for elections that all member states must follow.

Such a framework could include regular penetration testing, real-time monitoring for cyber threats, minimum encryption requirements, and the use of offline backups for vote counting.
The European Union Agency for Cybersecurity (ENISA) could take a leading role in supporting national governments with technical expertise and funding for capacity building.
At the national level, governments should establish dedicated election cybersecurity task forces that work with intelligence services and civil society.
This solution addresses the technical vulnerabilities that foreign actors often exploit and helps restore public confidence in the integrity of elections.