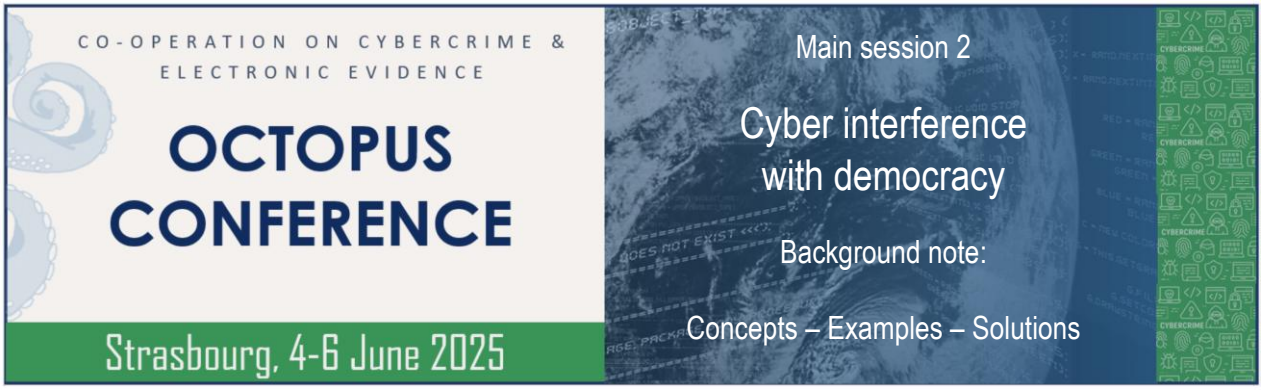


Alexander Seger
Head of Cybercrime Division
Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

Cyber interference with democracy: concepts

Concepts

2

Cyber interference with democracy: concepts

Democracy is a system of government where power is vested in the people, either directly or through elected representatives. Principles and processes of democracy include:

- Human rights and freedoms
- Elections (government of the people) that are universal, free, fair, equal, secret and held at regular intervals
- Political equality
- Government for the common public interest (government for the people)
- Separation of powers between the executive, the legislature and the judiciary.
- Rule of law. No arbitrary use of power. Nobody above the law. Everyone equal before the law
- Accountability
- Transparency
- Competition of political parties
- Pluralism of interests

3

Cyber interference with democracy: concepts

Elections are at the core of democracy. Principles to ensure elections are free, fair, and transparent, include:

- Universal suffrage
- Equal suffrage
- Direct elections
- Secret voting
- Freedom of expression and political pluralism
- Free and fair elections: Elections should be conducted fairly and impartially, ensuring that no candidate or group has an unfair advantage, and that the process is free from manipulation, fraud, or external interference
- Transparency: The election process, including the registration of voters, the conduct of voting, the counting of votes, and the financing of political candidates and parties and of election campaigns, should be open to public scrutiny
- Elections at regular intervals

4

Cyber interference with democracy: concepts

Cyber interference with democracy refers to the use of information and communication technologies to undermine or manipulate democratic institutions and processes as well as public opinion and trust in democratic governance.

The goal of cyber interference is often to weaken confidence and trust in elections and in democracy in general, to distort the results of elections and other democratic processes in favour of particular candidates or parties or to manipulate public opinions for political, economic or ideological gain.

Given the central role of elections in democracies, "cyber interference with democracy" often takes the form of interference with elections and election campaigns, through:

- Cybercrime
- Information operations (IO)

5

Cyber interference with democracy: concepts

Cybercrime, that is, offences against the confidentiality, integrity and availability of computer systems and data as well as computer-related forgery and fraud related to democratic processes and institutions, including elections and election campaigns.

Examples:

- Illicit access to computer systems in order to steal data from political candidates or election campaigns.
- Intercepting communications to obtain sensitive information. Interference with voter registration data, with results of votes or with voting machines.
- Data interference to damage voter data bases or alter results of votes.
- System interference such as distributed denial of service attacks or the use of malware to hinder the functioning of computer systems used in elections or campaigns.
- Forgery of websites, or of any information, including financial disclosures.
- Phishing attacks against persons involved in elections or campaigns to obtain access credentials or other confidential information.
- Deepfakes generated by artificial intelligence to deceive voters and influence public opinion.

See T-CY Guidance Note on "Aspects of election interference by means of computer systems covered by the Budapest Convention" (July 2019)

6

Cyber interference with democracy: concepts

Information operations (IO) aimed at manipulating public opinion and voter behaviour, causing or exploiting social and political divides, and at undermining trust in the results of elections and in democracy in general.

Examples:

- Creation of fake (synthetic) social media accounts and engagement to promote particular candidates or parties.
- Direct or micro-targeting of voters with IO materials.
- Amplification and dissemination of IO materials through social media and websites.
- Covert funding, advertisement of other forms of support to particular candidates or parties.
- Use of AI-generated deepfakes to deceive the public.
- Use of IO materials to encourage physical protests and violence, to exploit political and social divides, and to promote extremist candidates and positions.

These forms of interference may involve foreign influence operations.

7

Cyber interference with democracy: concepts

Note:

- Both categories – cybercrime and information operations – are interconnected. For example, information obtained through cybercrime may then be used in information operations ("hack and leak operations").
- Moreover, cyber interference does not take place in isolation but is often part of broader attempts of (domestic or foreign) interference with democracy, including elections.
- Governments in power may violate principles of democratic governance, and interfere with democracy / elections by removing checks and balances, misuse administrative resources during electoral processes, persecute or prosecute political opponents etc.

8

Violation of principles, laws and regulations

Such interference may violate principle of democracy and of free, fair and transparent elections as well as related domestic laws, rules and regulations, including, for example:

- Electoral integrity laws;
- Laws on electoral fraud and voter integrity;
- Laws regarding foreign influence and election interference;
- Laws and regulations on political financing;
- Anti-corruption laws;
- Criminal law provisions, including on cybercrime (offences against and by means of computer systems);
- Laws on information security;
- Data protection laws;
- Laws and regulations related to media and broadcasting.

9

Relevant standards

- Convention on Cybercrime and Protocols + T-CY Guidance Note on election interference
- Cybersecurity standards (e.g. NIS2 Directive (EU) 2022/2555)
- Digital Services Act (European Union, 2024) imposes obligations on digital platforms to combat illegal content, including election-related manipulation. Violations include:
  - Failure to Remove Disinformation: Platforms must promptly act against false content that undermines electoral integrity.
  - Non-Compliance with Transparency: Platforms must disclose how algorithms promote or demote political content.
  - Risk Mitigation Failure: Platforms must assess and address risks related to electoral integrity.
- Council of Europe / Venice Commission standards:
  - Council of Europe standards in the electoral field & Reference standards of the Council of Europe - Elections
  - Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence (December 2024)
  - Political parties and financing

10

Examples of cyber interference

Cyber interference with democracy is a global challenge

Some examples:

- **Brazil**: General elections in 2018 and 2020 were targeted by information operations, including disinformation that electronic voting systems have been interfered with to manipulate results.
- **Ghana**:
  - Cybercrime: Website of Electoral Commission hacked and defaced with misleading election results (2016)
  - IO: Elections targeted through disinformation about election results, fake endorsements of candidates etc. (2016 and 2020) and use of bots, synthetic accounts to amplify messages as well as AI-generated content and deep fakes to mislead voters and manipulate public opinion (2024).

Cyber interference with democracy: examples

Cyber interference with democracy is a global challenge

More examples:

- **Philippines:**
  - Cybercrime: Extraction of the entire vote database (55 million voters) and leaking of information (2016). DDOS attacks against independent media and fact-checking services (2021-2022).
  - IO: mis- and disinformation through synthetic accounts, bots and troll farms (2016, 2022). "Digital proxy warfare" with covert influence operations (influencers and troll armies) and disinformation.

- **USA:**
  - Cybercrime: Illegal access to computer systems of the Democratic National Committee and theft and subsequent dissemination of sensitive information by the Russian military intelligence agency, GRU (2016). Election systems in all 50 States targeted but no alteration of data reported (2016). Computer systems again targeted in 2020 and 2024, but no breaches reported.
  - IO: Coordinated social media campaigns through fake accounts and troll farms (Internet Research Agency in Russia), information operations (2020, 2024) as well as use of AI-generated deepfakes by foreign actors (2024).

13

Cyber interference with democracy: examples

Cyber interference with democracy: Example of Ukraine 2014 and 2019

- Ukrainian presidential elections 2014:
  - Cybercrime: Large-scale attacks against election infrastructure. Espionage and phishing attacks against election officials.
  - IO: publication of false election results and other disinformation campaigns
  - Main actors: Russian intelligence services (APT 28 and Sandworm of GRU, APT 29 of SVR) and groups linked to GRU and FSB (Cyber Berkut).

- Ukrainian presidential elections March/April 2019:
  - Cybercrime: Pre-election attacks (starting mid-2018) by APT28 and APT29 against government networks. Election infrastructure and media websites attacked by APT28, Sandworm and APT29 in 2019. More attacks after the elections.
  - IO: Fake accounts and bots for false polls and surveys and large-scale disinformation

- Cyber interference accompanied by covert funding of pro-Russian candidates, attempts of bribery and discrediting of election results in Russian media as well as physical violence in Donbass.

14

Cyber interference with democracy: Example of Moldova 2024*

- Cybercrime:
  - Illegal access to computer systems of electoral bodies and political parties.
  - Website defacement and other data interference.
  - DDOS attacks and other system interference against systems for election management, websites and similar.
  - Phishing and other social engineering targeting election officials and others to obtain access credentials.

- IO:
  - Social media manipulation through synthetic accounts, bots and troll farms to rapidly spread and amplify disinformation, divisive narratives and propaganda.
  - Micro-targeting to deliver tailored disinformation to specific segments of the population.
  - Coordinated release of disinformation and exploitation of social divides.

Actors reportedly included Russian intelligence services and groups linked to them, as well as local pro-Russia actors.
Cyber interference was accompanied by propaganda and disinformation by Russian state media (e.g. RT and Sputnik News).

*Presidential elections of 20 October and 3 November 2024

15

Cyber interference with democracy: examples

Cyber interference with democracy: Example of Romania 2024*

- Cybercrime:
  - DDOS and other attacks (85,000) against government and election-related websites.
  - Phishing and other social engineering attacks against election and other officials to obtain access credentials.

- IO:
  - Social media manipulation with false narratives, fake news outlets, deepfake videos and use of inauthentic accounts and bots to amplify disinformation and social divisions.
  - Network of some 25,000 accounts on TikTok as well as influencers funded and coordinated by foreign actors.

Aggressive hybrid attacks attributed to Russian state actors combined with financing from undisclosed sources to promote one particular candidate, manipulate public opinion and destabilise the electoral process.

* 24 November 2024 first round of presidential elections, parliamentary elections 1 December 2024. Presidential elections then cancelled by Constitutional Court and postponed to May 2025

16

Cyber interference with democracy: Example of Germany 2025*

- IO:
  - Disinformation by 100+ Russia-linked websites spreading AI-generated disinformation attacking pro-European politicians and favouring the right-wing AfD (January 2025).
  - Social media manipulation through troll farms and botnets to amplify divisive content and polarise public opinion.
  - Publication of fabricated opinion polls, coordinated release of deepfake videos and disinformation with claims of election fraud and voter suppression.

Much of these IO have been attributed to “Storm-1516”, a Russian group that is considered to be an offshoot of the former Internet Research Agency.

Cyber interference with these elections was accompanied by other forms of interference, including acts of sabotage by individuals recruited by Russia.

Additional concerns of algorithmic bias or “tweaking” by X (former Twitter) in favour of the right-wing AfD.

* 23 February 2025 General election to the Federal Parliament

17

Violation of what rules?

18

Example of Moldova

- Electoral Code of the Republic of Moldova (2016)
  - Article 37 – Equal Rights of Candidates
  - Article 55 – Campaigning in Media
  - Article 59 – Prohibition of Foreign Influence on Electoral Process
- Criminal Code of the Republic of Moldova
  - Article 182 – Electoral Fraud
  - Article 338 – Influence on the Electoral Process
  - Articles 259 – 260 (cybercrime)
- Law No. 71/2007 on the Protection of Personal Data
- Law No. 164/2005 on Information Security
- Law No. 26/2008 on the Broadcasting Code
- Law No. 112/2014 on the Regulation of Internet Services
- Law No. 132/2016 on the Prevention and Combating of Corruption

19

Examples of laws, rules or regulations that may be affected

Example of Romania

- Electoral Code
- Criminal Code
  - Articles on cybercrime
  - Articles on election fraud and manipulation
- Law no. 334/2006 on the financing of political parties' activity and electoral campaigns (amended 2015)
- Media regulations

20

Examples of laws, rules or regulations that may be affected

Example of Germany

- Electoral Code
- Law on political parties
- Criminal Code
  - Articles on cybercrime
  - Articles on election fraud and manipulation (paragraphs 107 – 108b)
- Telemedia Act

21

Cyber interference with democracy: Note

Cyber interference with democracy in Europe:

- Not in isolation, part of multi-pronged campaigns
- May peak around elections, but comprise longer-term effort
- State and non-state actors, dividing lines not always clear

22

Cyber interference with democracy: Actors

Cyber interference with democracy in Europe by:

- Governments in power, domestic candidates, parties or groups (often pro-Russia or Russia supported)
- Units of Russian intelligence services (Military intelligence – GRU (e.g. APT 28 and Sandworm/APT 44), Federal Security Service – FSB, Foreign Intelligence Service – SVR (e.g. APT 29)
- Cybercrime groups and disinformation networks – often aligned with Russian intelligence services – such as Coldriver, Killnet, Storm-1516 , Storm-1679
- Russian State media (RT, Sputnik News)
- APTs linked to China and Iran

Role of social media platforms (X, Telegram, TikTok, Facebook, Instagram etc.)?

23

Cyber interference with democracy: Actors?

Role of social media platforms?

Use of social media platforms for automated disinformation and election interference through:

- Troll farms and influence networks
- Deepfake and AI-generated personas / accounts
- Bot-fueled content amplification/virality
- Hashtag hijacking and coordinated trends
- Cross-platform laundering
- Coordinated inauthentic behaviour (CIB)

Facilitated by	Impact
Weak identity verification and enforcement	Easy to create botnets, fake accounts or impersonate individuals
Algorithm-driven virality	Amplifies fake content with high engagement
Emphasis on short-form emotion	Easier to manipulate public opinion rapidly
Lax cross-platform detection	Enables influence laundering between platforms
Insufficient collusion detection	Permits coordinated inauthentic behaviour (CIB) to remain under the radar
Delayed moderation and takedown	Allows disinformation to spread before removal
Limited transparency and reporting	Hard for researchers to track state-linked ops

24

Solutions?

Solutions?

Counter disinformation through a combination of measures, e.g.:

- Obligations for social media platforms (regulation / self-regulation / codes of conduct)
- Media literacy
- Fact-checking

Clear rules, transparency and communication to ensure trust and legitimacy

Make ("analogue") rules governing elections and election campaigns more effectively applicable to the digital environment

Strengthen measures to prevent cyber interference with elections, including:

- Cybersecurity measures
- Monitoring, threat intelligence and incident response

More effective criminal justice and national security measures against cyber interference, also by foreign actors, including:

- Enforce laws on cybercrime domestically and cooperate internationally
- Make use of the Convention on Cybercrime and Second Protocol on e-evidence
- Capacity building to gather intelligence, investigate and prosecute cyber interference with democracy/elections

Cyber interference with democracy: what solutions?

Make ("analogue") rules governing elections and election campaigns more effectively applicable to the digital environment

For example:

- Stronger digital transparency requirements (disclosure of political ads; digital "imprint" laws identifying sponsors of political content; platforms to maintain public databases of political ads, etc.)
- Regulation of online mis- and disinformation (detection and take-down by platforms etc.)
- Fairness in algorithmic amplification (audit and transparency of algorithms prioritising political content, etc.)
- Enforce rules on political financing in the digital environment
- Digital campaign finance reform (cover virtual assets and decentralise funding; reporting on digital ad and micro-targeting expenditure; spending limits for digital political campaigns)
- Data protection and voter privacy (informed consent for micro-targeting based on personal data)
- International and cross-platform cooperation on election integrity
- Stronger enforcement mechanisms (digital election watchdogs to monitor compliance; empower swift action by regulators; expedited removal of disinformation by platforms)

27

Cyber interference with democracy: what solutions?

- Fairness in algorithmic amplification (audit and transparency of algorithms prioritising political content, etc.) …

POLITICO

Var in Ukraine | Newsletters | Podcasts | Poll of Polls | Policy news | Events

NEWS > TECHNOLOGY

X challenges German court decision that forces it to share election data

SHARE

FEBRUARY 17, 2025 4:57 PM CET
BY ELIZA GKRITSI AND CHRIS LUNDAY

Elon Musk's X has challenged a German court decision that instructed the platform to share data with researchers, the court confirmed to POLITICO.

In an urgent injunction, the Berlin Regional Court last Thursday instructed X to share real-time access to the data on the upcoming German elections via its online interface until Feb. 25.

28

Cyber interference with democracy: what solutions?

Strengthen measures to prevent cyber interference with elections

For example:

- Strengthen security of election and campaign infrastructure (cybersecurity measures, consider election systems "critical infrastructure" (see IDEA 2019, ENISA 2019, NIS2 2022))
- Countering disinformation (social media regulation, fact-checking initiatives, public awareness, digital literacy)
- Enhancing monitoring, threat intelligence and incident response (real-time threat detection; rapid response teams; public/private cooperation)
- Improved transparency in online political advertising (platforms to label political ads, including funding sources and target audience; algorithmic accountability and transparency regarding political content)
- Establish multi-stakeholder groups or similar to monitor compliance with rules on election campaigns, including political funding in relation to specific elections
- Consider use of artificial intelligence to prevent, identify and counter cyber interference

29

Cyber interference with democracy: what solutions?

More effective criminal justice and national security measures against cyber interference, including by foreign actors

For example:

- Enforce laws on cybercrime domestically and cooperate internationally. Make use of the Convention on Cybercrime and Second Protocol on e-evidence
- Capacity building to gather intelligence, investigate and prosecute cyber interference with democracy/elections
- Follow the money/virtual assets: search, freeze and confiscate assets related to election interference
- Tracking and countering foreign information operations by security services
- Diplomatic, economic and cyber countermeasures against foreign actors

30

Cyber interference with democracy: what solutions?

Take combination of measures to counter disinformation not only in relation to cyber interference with democracy

Carnegie Endowment for International Peace (2024): Countering disinformation effectively – An evidence-based policy guide (Jon Bateman / Dean Jackson)

Type	Intervention	How much is known?	How effective does it seem?	How easily does it scale?
	1. Supporting local journalism	Modest	Significant	Difficult
	2. Media literacy education	Significant	Significant	Difficult
	3. Fact-checking	Significant	Modest	Modest
	4. Labeling social media content	Modest	Modest	Easy
	5. Counter-messaging strategies	Modest	Modest	Difficult
	6. Cybersecurity for elections and campaigns	Modest	Modest	Modest
	7. Statecraft, deterrence, and disruption	Modest	Limited	Modest
	8. Removing inauthentic asset networks	Limited	Modest	Modest
	9. Reducing data collection and targeted ads	Modest	Limited	Difficult
	10. Changing recommendation algorithms	Limited	Significant	Modest

Public information · Government action · Platform action

31

Cyber interference with democracy: what solutions?

Role of social media platforms

► solutions?

32

Cyber interference with democracy: what solutions?

European Commission

EN | Search

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office

Home > Library > The Code of Conduct on Disinformation

https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

POLICY AND LEGISLATION | Publication 13 February 2025

The Code of Conduct on Disinformation

The Code of Conduct aims to combat disinformation risks while fully upholding the freedom of speech and enhancing transparency under the Digital Services Act (DSA).

On **13 February 2025**, the Commission and the European Board for Digital Services endorsed the official integration of the voluntary Code of Practice on Disinformation into the framework of the Digital Services Act (DSA).

The Code of Practice on Disinformation is a pioneering framework agreed upon by a broad range of stakeholders - online platforms, search engines, the advertising industry, fact-checking, and civil society organisations, etc. Established in 2018, it was significantly strengthened in 2022, with the

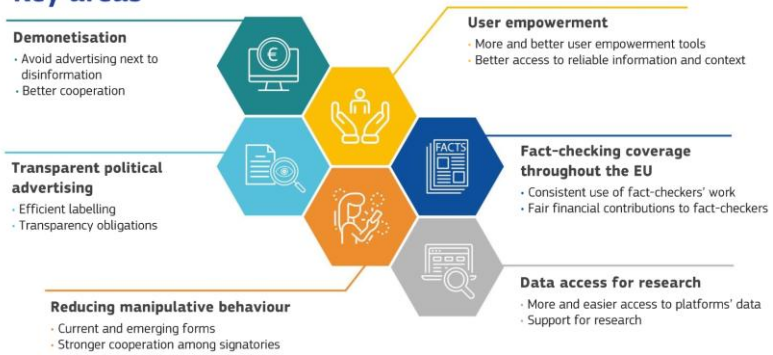
iStock GettyImages © PerlaStudio

33

Cyber interference with democracy: what solutions?

Code of Conduct on Disinformation

Key areas



The 42 Signatories*

Major Online Platforms and Search Engines: Google (for Google Advertising, Search and YouTube), Meta (for Facebook, Instagram, Messenger and WhatsApp), LinkedIn, Microsoft Ads, Microsoft Bing, TikTok and trade organisation DOT Europe

Smaller/specialised Online Platforms: Twitch, Vimeo, Seznam, The Bright App

Advertising industry: European Association of Communication Agencies (EACA) Interactive Advertising Bureau (IAB Europe), DoubleVerify, Ebiquity.

Fact-checkers: Demagog, European Fact-Checking Standards Network (EFCSN), Faktograf, Maldita, Newtral, Pagella Politica, Science Feedback.

Civil Society/research organisations: Alliance4Europe, Avaaz, Globsec, Democracy Reporting International (DRI), Debunk EU, CEE Digital Democracy Watch FIDU (Italian Federation for Human Rights), Les Surligneurs, Reporters without Borders (RSF), VOST Europe, WhoTargetsMe.

Players offering technological solutions: ActiveFence, Adobe, AI Forensics, Resolver (formerly Crisp), Legitimate, Logically, NewsGuard, Valid (formerly the Daily Ledger), the Global Disinformation Index (GDI).

https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

34

Code of Conduct on Disinformation

Within the framework of the Digital Services Act

Table of Contents

https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

35

Code of Conduct on Disinformation

Example

Common understanding of impermissible manipulative behaviour

Commitment 14. In order to limit impermissible manipulative behaviours and practices across their services, relevant Signatories commit to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviours, actors and practices not permitted on their services.

Such behaviours and practices, which should periodically be reviewed in light of the latest evidence on the conducts and TTPs employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework, include:

- The creation and use of fake accounts, account takeovers and bot-driven amplification,
- Hack-and-leak operations,
- Impersonation,
- Malicious deep fakes,
- The purchase of fake engagements,
- Non-transparent paid messages or promotion by influencers,
- The creation and use of accounts that participate in coordinated inauthentic behaviour,
- User conduct aimed at artificially amplifying the reach or perceived public support for disinformation.

https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

36

Cyber interference with democracy: what solutions?

Code of Conduct on Disinformation

Example

In order to satisfy Commitment 14:

Measure 14.1. Relevant Signatories will adopt, reinforce and implement clear policies regarding impermissible manipulative behaviours and practices on their services, based on the latest evidence on the conducts and tactics, techniques and procedures (TTPs) employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework.

QRE 14.1.1: Relevant Signatories will list relevant policies and clarify how they relate to the threats mentioned above as well as to other disinformation threats.

QRE 14.1.2: Signatories will report on their proactive efforts to detect impermissible content, behaviours, TTPs and practices relevant to this commitment.

Measure 14.2. Relevant Signatories will keep a detailed, up-to-date list of their publicly available policies that clarifies behaviours and practices that are prohibited on their services and will outline in their reports how their respective policies and implementation address the above set of TTPs, threats and harms as well as other relevant threats. Such information will also be reported in the Transparency Centre. The list of TTPs will serve as the base for the TTPs to be reported upon and relevant Signatories will work within the permanent Task-force to further develop and refine related indicators on the impact/effectiveness of their related actions. Relevant Signatories will also develop further metrics to estimate the penetration and impact that fake/inauthentic accounts have on genuine users and report at Member State level (including trends on audiences targeted; narratives used etc.).

QRE 14.2.1: Relevant Signatories will report on actions taken to implement the policies they list in their reports and covering the range of TTPs identified/employed, at the Member State level.

https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

37

Cyber interference with democracy: what solutions?

Code of Conduct on Disinformation

- Transparency Reports

https://disinfocode.eu/reports

Google	March 2025	25 Mar 25	2025
Meta	March 2025	25 Mar 25	2025
Microsoft	March 2025	25 Mar 25	2025
TikTok	January 2023	14 Mar 25	2023
TikTok	July 2023	14 Mar 25	2023
TikTok	March 2024	14 Mar 25	2024
TikTok	September 2024	14 Mar 25	2024
twitch	January 2023	14 Mar 25	2023
twitch	March 2024	14 Mar 25	2024
twitch	September 2024	14 Mar 25	2024
	January 2023	14 Mar 25	2023

38

Cyber interference with democracy: what solutions?

Code of Conduct on Disinformation

▶ Transparency Reports

https://disinfocode.eu/reports

GOOGLE Transparency Report March 2025
Submitted
Executive summary

Google's mission is to organise the world's information and make it universally accessible and useful. To deliver on this mission, elevating high-quality information and enhancing information quality across our services is of utmost importance.

As the EU Code of Practice on Disinformation is being brought under the EU Digital Services Act (DSA) framework, Google has revised its subscription to focus on reasonable, proportionate and effective measures to mitigate systemic risks related to disinformation that are tailored to our services. Accordingly, Google has exited certain commitments that are not relevant, practicable or appropriate for its services, including all commitments under the Political Advertising and Fact-Checking chapters.

39

Cyber interference with democracy: what solutions?

TikTok

Code of Practice on Disinformation – Report of TikTok for the period 1 July 2024 - 31 December 2024

Transparency Center

Reporting on the signatory's response during an election

2024 Romanian Presidential Election

Threats observed during the electoral period: [suggested character limit 2000 characters].

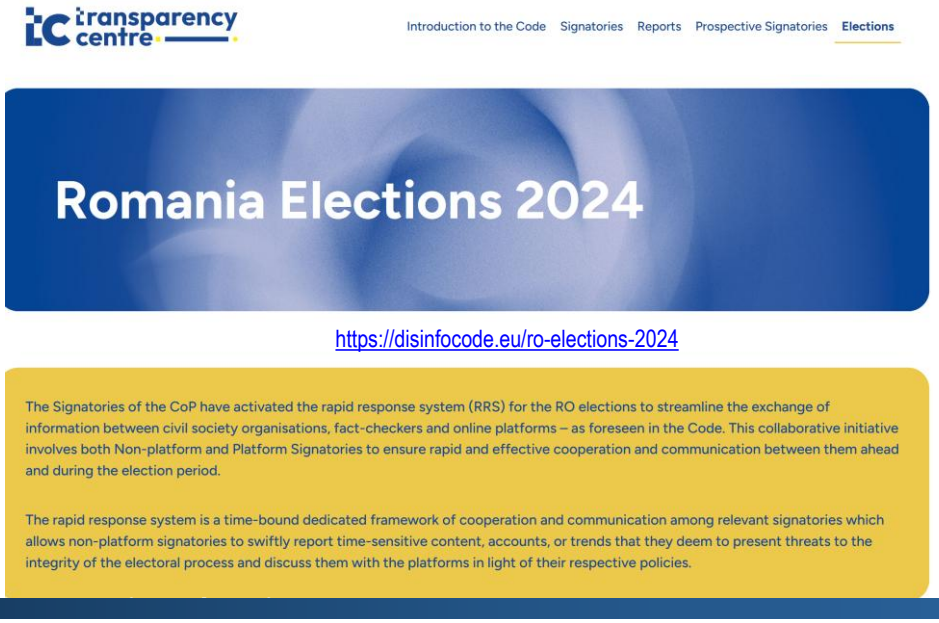
As co-chair of the Code of Practice on Disinformation's Working Group on elections, TikTok takes our role of protecting the integrity of elections on our platform very seriously. We have comprehensive measures in place to anticipate and address the risks associated with electoral processes, including the risks associated with election misinformation in the context of the Romanian Election which took place on 24 November 2024.

The following are examples of some of the threats TikTok observed in relation to the Romanian Presidential Election:

- TikTok reported removing six CIO networks in 2024 that were identified as specifically targeting a Romanian audience. More information relating to the network disruptions is published on our dedicated Covert Influence Operations transparency page.
- In addition to these networks, it's worth highlighting our broader defences against covert influence campaigns across Europe. In September 2024, we took global action against a covert network linked to Sputnik Media. When we remove such networks, we continue monitoring for any attempts to re-emerge. As part of our anti-recidivism strategy, we removed 11 accounts in November 2024 believed to be associated with Sputnik Media and targeting Romanian and Moldovan audiences.
- We proactively removed more than 5,500 pieces of election-related content in Romania for violating our policies on misinformation, harassment, and hate speech since the end of October.
- We received 11 notifications through the COPD Rapid Response System in relation to the Romanian Presidential Election, which were rapidly addressed. Actions included banning or geo-blocking of accounts and content removals for violation of Community Guidelines.

40

Cyber interference with democracy: what solutions?



41

Cyber interference with democracy: what solutions?

- How to reconcile countering disinformation and holding platforms accountable with the freedom of expression?
- How to counter election interference if governments in power are not or are not perceived as neutral?
  - Multi-stakeholder monitoring/response models
  - Transparency in communication to the public

42

Cyber interference with democracy: what solutions?

- When is an interference that severe that an election becomes invalid or is cancelled?

► Urgent report of the Venice Commission (January 2025)

43

Cyber interference with democracy: what solutions?

Venice Commission: Urgent Report on the Cancellation of Elections by Constitutional Courts (January 2025)

A. Decisions to cancel election results should be taken by the highest electoral body and such decisions should be reviewable by the highest judicial body, the constitutional court or a specialised electoral court when such a judicial body exists [para. 21];

B. The power of constitutional courts to invalidate elections ex officio – if any – should be limited to exceptional circumstances and clearly regulated [para. 27];

C. The cancellation of a part of elections or elections as a whole can be allowed only under very exceptional circumstances as ultima ratio and on the condition that irregularities in the electoral process may have affected the outcome of the vote [paras 18 and 39];

https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-PI(2025)001-e

44

Cyber interference with democracy: what solutions?

D. The decision-making process concerning election results must be accompanied by adequate and sufficient safeguards ensuring, in particular, a fair and objective procedure and a sufficiently reasoned decision based on clearly established facts which prove irregularities that are so significant that they may have influenced the outcome of the election; affected parties must have the opportunity to submit their views and evidence, and the discretion of the judge considering election matters should be guided and limited by conditions set out in the law; decisions must be taken within reasonable time-limits [paras 16, 28, 31, 33];

E. It should be possible to challenge election results based on violations of electoral rights, freedoms and interests by the State, public and private electoral stakeholders, and on influence of the media, and of social media in particular, including those sponsored and financed from abroad [paras 48 and 49];

45

Cyber interference with democracy: what solutions?

F. States should regulate the consequences of information disorders, cyber-attacks and other digital threats to electoral integrity; candidates and parties must be granted fair and equitable access to online media, and regulations should be implemented to ensure that artificial intelligence systems by internet intermediaries do not favour certain parties or candidates over others [paras 54 and 55];

G. The general rules on campaign finance and transparency should be applied to online campaigning using social media platforms; States should also regulate that online electoral advertising must be identified as such and must be transparent, and that social media platforms are required to disclose data on political advertising and their sponsors [paras 56 and 58].

https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-PI(2025)001-e

46

Cyber interference with democracy: discussion

Q & A