

# Mapping and remedying vulnerabilities in the EU's critical infrastructure

## Election infrastructure and electoral integrity

### ABSTRACT

This briefing provides background information for the members of the Special committee on the European Democracy Shield (EUDS) on election infrastructure vulnerabilities to foreign interference and on corresponding countermeasures. The briefing focuses on the criticality of election infrastructure and on safeguarding electoral integrity, also in light of the approach set out in the Commission's Communication on the European Democracy Shield. Moreover, the paper considers the role of private sector election interference services.

The briefing begins with an introduction to the different components of election infrastructure and general information on the conduct of elections. It continues with an overview of the election infrastructure interference threat landscape, taking the findings of the European Union Agency for Cybersecurity (ENISA) into account. It then examines recommendations provided by the European Cooperation Network on Elections to mitigate these threats. Next, the briefing presents a section on critical infrastructure legislation and on the measures outlined in the European Democracy Shield to protect election infrastructure.

This briefing has been prepared internally by the European Parliament's Policy Department for Justice, Civil Liberties and Institutional Affairs at the request of the EUDS Committee.

### Introduction

Protecting the integrity and smooth conduct of elections, free from interference, is vital to ensuring that citizens can exercise their [right to vote](#). It is also crucial for trust in election results. Today, digital components have become an integral part of election infrastructure. While digitalised election systems can offer significant advantages, their use can also create a degree of vulnerability to emerging threats.

EU Member States have digitalised their electoral infrastructures to varying degrees. For instance, in Estonia, online voting has been possible for 20 years. Estonia is the only EU country that allowed e-voting in the [2024 EU elections](#). Another interesting case is France, where voters living abroad can vote online in [General and Consular elections](#) (for advisors representing French nationals abroad). Other EU Member States have also made progress in digitalising their election infrastructures. [Research](#) from the European Union Agency for Cybersecurity ([ENISA](#)) indicates that technology is mostly used by EU Member States for voter registries or the transmission and display of election results.



These advancements lead to a strong focus on cybersecurity. The public sector is one of the [top 5 targets](#) for cyber-attacks in the EU, with ransomware being the most impactful cyber threat in 2025. There is concern that malign actors could attempt to manipulate election outcomes, for instance by deleting or altering votes within technical systems. Another form of interference could entail disabling public websites that provide polling information, thereby deliberately disrupting the conduct of elections. To shield against interference, a high level of cybersecurity is necessary. This entails regular updating of equipment, maintenance and technical support.

The EU Member States are responsible for the organisation and the conduct of elections. Of course, the European elections add a [Union dimension](#), as European political parties and their associated foundations play a central role in European election campaigns. While actions in the context of running elections remain the primary responsibility of Member States, the [European Cooperation Network on Elections](#) supports mutual assistance among Member States. This network consists of national authorities responsible for electoral matters. In the [European Democracy Shield](#), published on 12 November 2025, the Commission proposed strengthening its support for Member States under the European Cooperation Network on Elections to enhance electoral integrity and preparedness. The Commission stated that there “is a need to better protect electoral processes, including the election-related infrastructure, from attacks combining FIMI and disinformation campaigns and a range of other tools and tactics, such as cyber-attacks, covert campaign financing, vote buying, attacks against political candidates, attempts to instigate social unrest or acts of violence and destabilisation”.

Interference threats related to elections can be grouped into three main categories: physical threats, cyber threats and disinformation threats. This briefing primarily focuses on threats to the physical and digital election infrastructure.

## Vulnerabilities in election infrastructure

Several elements of election infrastructure could be vulnerable to election interference. This section first outlines several examples of how technology is used in the electoral process in order to illustrate how such tools and systems may function in practice. The examples outlined include official election information websites, vote capture devices, election management systems and vote tabulation systems. This section also analyses cyber threats, physical threats and the role of private sector interference services in this regard.

### Official election information websites

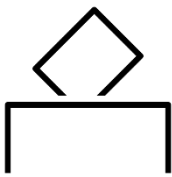


During election periods, governments of EU Member States usually provide election-related information on official websites. This information can include the date of the election, the voting system, voting modalities (in-person, postal, online) and other relevant information. It is of the utmost importance that citizens know when, how and where they can vote. These websites also often provide election results after the vote or even real-time calculations and updates.

Government websites have been prominent targets of malicious hacker attacks in the past. [Hacktivists](#) are hacker activists who attempt to gain unauthorised access to computer files or networks in order to further social or political ends. Rendering government websites unavailable can hinder citizens’ participation in elections, as they might be unable to access important election information. Malicious attacks on websites often occur in the form of [Distributed Denial of Service](#) (DDoS) attacks. These DDoS attacks can be defined as hackers’ attempts to overload a website or network until its performance decreases or becomes unavailable. Hacktivists can also attempt to alter websites to display incorrect voting information or election results.

Shortly before and throughout the 2024 European Parliament elections, a pro-Russian hacktivist group targeted interior and foreign affairs portals in 14 Member States, according to ENISA's '[Sectorial Threat Landscape – Public Administration](#)', published on 6 November 2025. Malicious hacktivists also targeted more than 40 Austrian entities, including government websites, airports, financial services and the Vienna Stock Exchange, in a further DDoS case during the Austrian parliamentary elections in 2024. In the report's Outlook, ENISA emphasised that it "is highly likely that DDoS campaigns will continue, especially around key events such as elections or summits, without causing significant operational disruptions". The Austrian case highlights that these attacks are not necessarily limited to government websites but can also attempt to sow chaos in other fields, such as transport or financial services. A [Commission Memo](#) of October 2024 explained that during the 2024 European Parliament elections, minor cybersecurity incidents were recorded, mostly in the form of DDoS attacks led by pro-Russian hacktivist groups, but these did not have a significant impact on the election.

### Vote capture devices



Before digitalisation, casting a ballot had to be done in-person using pen and paper. Now, more options are available. With e-voting, voters authenticate and cast their ballots online. [International IDEA](#) lists accessibility and inclusiveness among the advantages of e-voting. It facilitates participation for voters with limited mobility. However, the institute also explains that e-voting involves ballot-casting from uncontrolled environments, potentially giving rise to concerns. Voter authentication is crucial to uphold the integrity of e-voting. [Estonia](#) handles voter authentication via a voter app (downloaded from the election website), using electronic ID card authentication. Under this system, voting is exercised via the citizen's own computer.

In addition to e-voting, electronic voting machines can also be used in physical voting stations. These are called Direct Recording Electronic (DRE) voting machines, as they can record the vote directly in electronic form. These machines allow for citizens to participate in the election in-person, in a controlled environment, while still capturing the vote digitally. Regarding the use of electronic voting machines in polling stations, the [Council of Europe](#) recommended in 2017 the use of paper ballots as a second medium to enable verification of the vote later. These electronic voting machines allow [for automated ballot counting](#). Another mixed solution would be to use an electronic ballot scanner for paper ballots.

Researchers from the French National Institute for Research in Digital Science and Technology ([INRIA](#)) and the [PESTO](#) project [underlined](#) two guarantees when it comes to the security of electronic voting: confidentiality of the vote and integrity of the result. They stated that "the result declared must correspond to the sum of the ballots submitted (with no ballot altered or removed) and these ballots must have been sent in by legitimate voters."

### Election management systems

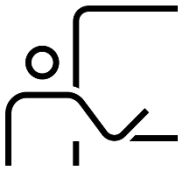


Electronic election management systems are often at the core of election infrastructure, even if the vote is conducted on paper in polling stations. Software is needed to operate electronic voting machines in polling stations. Moreover, electronic election management systems can be used to aggregate votes and calculate election results. Even in the cases where paper ballots are tallied centrally, an electronic software is often used to support the counting.

The Non-Paper from the Commission Services "[Compendium of e-voting and other ICT practices](#)" of 2023 illustrates the software systems and technological solutions used in Romania to enhance electoral integrity. A web-based voter register is used in Romania, as well as an electronic system for monitoring turnout and preventing illegal voting and an electronic tabulation system. The report explains that the Romanian election monitoring system allows for audio and video recording of the vote-counting process, and creates and

stores results protocols. It also checks data correlations in the results protocols and transmits results to the tabulation system.

### Vote tabulation systems



After individual votes are recorded, they must be transmitted and tabulated in order to determine the voting results. The [International IDEA's information and communication technologies in elections database](#) indicates that 21 EU Member States process election results through the use of an electronic tabulation system. Half of the Member States enter results into e-tabulation systems between polling station level and central level.

According to this data, entering results into e-tabulation systems at the central level only is rare.

Electronic vote tabulation can offer significant [advantages](#), such as preventing cases of human error. It can lead to higher efficiency and faster reporting of preliminary results. However, technological solutions are not infallible, they require sound security measures and safeguards.

The examples of official election information websites, vote capture devices, election management systems and vote tabulation systems show that solid cybersecurity and precautionary measures are necessary to protect today's election infrastructure from potential threats.

### Cyber threats to election infrastructure

The ENISA Executive Director, Juhan Lepasaar, [highlighted](#) before the 2024 European Parliament elections that "reliability of the EU electoral processes depends on cyber secure infrastructures and on the integrity and availability of information. We must assess the new challenges, enhance preparedness and ensure the protection of our democracies". ENISA [argues](#) that rapid developments in Artificial Intelligence<sup>1</sup> (AI) have amplified cyber threats to election infrastructure due to the increased occurrence of deep fakes, the activity of hackers-for-hire and the growing sophistication of threat actors.

The [NIS Cooperation Group](#), composed of representatives of EU Member States, the Commission and ENISA, published a [Compendium on Elections Cybersecurity and Resilience](#) on 6 March 2024. This Compendium offers an overview of possible cybersecurity threats in the context of elections:

- ransomware and attacks seeking to render voters' registration data unavailable, hence disrupting the conduct of elections;
- DDoS attacks;
- social engineering and phishing attacks that provide access to sensitive voter information used to target misleading messages, or to exfiltrate internal party or governmental documents;
- website defacement, for instance altering the content of public websites with election-related information;
- cybersecurity attacks facilitating the creation and spread of manipulated information;
- and supply-chain attacks, meaning malicious actors targeting suppliers of hardware and software used in election infrastructure.

In the context of supply-chain attacks, the authors highlight that "electoral infrastructure is vulnerable to these types of attacks because of its reliance to externally sourced components and services, also including commercial-off-the-shelf hardware and software". The authors of the Compendium also argue that the

<sup>1</sup> In the [European Democracy Shield](#), published on 12 November 2025, the Commission announced that it will further collaborate with Member States and stakeholders to come up with a guidance on the "fair, transparent, human-centred and responsible use of AI in electoral processes".

threat of cyber-attacks during elections can undermine trust, even if they were unsuccessful or did not even take place. According to ENISA, this is because alleged cyber-attacks against public institutions can add legitimacy to forged documents.

### Physical threats to election infrastructure

Physical attacks on election infrastructure have become a central concern to the integrity and the conduct of elections, according to the European Centre of Excellence for Countering Hybrid Threats' ([Hybrid CoE report](#) "Countering hybrid threats to elections: From updating legislation to establishing collaboration networks" of March 2024. These can range from small disruptions to bomb threats and direct physical attacks. For example, three polling stations in Poland received [bomb alerts](#) during the Polish parliamentary elections in October 2023, which led to the evacuation of around 200 people.

Other [physical threats](#) to election infrastructure include unauthorised access to polling stations and counting centres by malicious actors seeking to manipulate voting or counting, the disruption of essential services (power, water, transport) and disruptions in the accessibility of voting facilities and materials.

Natural hazards, such as floods and cyclones, can have a negative impact on electoral integrity, leading to a decrease of election-related media coverage, according to International IDEA's ["Electoral Risks" report](#) of September 2024. Media outlets and independent journalists might be forced to operate at a reduced capacity during natural hazards. At the same time, natural disasters offer a fertile ground for decreased equality of contestation, according to the report: In states where incumbents have control over state media, a declared emergency could lead to a 'lockdown' of opposition parties. It also warns that "emergency relief efforts may involve donations and humanitarian aid becoming misused for buying votes".

### The role of private sector interference services

Interference-as-a-service is an emerging area in which criminals can make profits in an increasingly polarised world. State-sponsored proxies are on the rise. Malicious threat actors increasingly use non-state actors as their proxies to carry out hybrid attacks. [Hybrid CoE](#) researchers explain that these non-state actors can take many forms, including private corporations. According to the Hybrid CoE report ["Countering state-sponsored proxies: Designing a robust policy"](#) of February 2025, by using such non-state actors to carry out hybrid threats, sponsors can benefit from their specialist knowledge while denying involvement.

These non-state threat actors can operate in different fields. The ENISA report ["ENISA Threat Landscape for DoS Attacks"](#), published on 6 December 2023, highlights that the increasing availability of DDoS-for-hire services by cybercriminals has played a role in the surge in denial-of-service attacks. The authors estimate that 66% of the attacks recorded were motivated by political or activist agendas. The authors also explain the appeal of denial-of-service attacks to threat actors: they require a low skillset, limited tools, allow the attackers to remain anonymous and can have a very noticeable impact.

According to the Hybrid CoE report ["Handbook on the role of non-state actors in Russian hybrid threats"](#) of December 2025, non-state actors are increasingly involved in propaganda and disinformation operations. These non-state actors can take the form of private-sector entities, such as public relations and IT companies. They provide interference infrastructure and complicate the attribution of an attack. Propaganda and disinformation non-state actors present themselves externally as independent from any state. The authors of the report argue that these non-state actors, including public relations agencies, play a crucial role in creating and managing digital media operations to disseminate pro-Kremlin narratives. "PR agencies have become key enablers of Russia's information confrontation and are directly curated by the Presidential Administration. They frequently collaborate with other private entities, such as IT companies, to build the digital infrastructure required for proxy websites."

A prominent example of a private sector election interference service was uncovered by the journalist consortium "[Forbidden Stories](#)" in the 'Team Jorge files'. According to information obtained by investigative journalists, this company was involved in election-manipulation-for-hire practices. The company offered services such as collecting intelligence, developing narratives and delivering these across platforms. On 25 May 2023, the ING2 and AFET Committees held a hearing on "[Election manipulation attempts](#)" to examine this case.

In this context, it is also worth mentioning the [Cambridge Analytica scandal](#) that came to light in 2018. Cambridge Analytica was a data analytics firm that harvested personal data of millions of Facebook users without their consent for [voter profiling and influencing](#) during the 2016 US presidential election and the 2016 pro-Brexit campaign.

## Overview of threat mitigation strategies

Threats to election infrastructure in EU Member States are increasing, requiring national authorities to remain vigilant against such interference. The [European Cooperation Network on Elections](#) has developed a [Risk Management Matrix for Elections](#), which was published in June 2025. The organisation and the conduct of elections are extremely complex. The European Cooperation Network on Elections argues that a thorough risk management strategy is key to safeguarding electoral integrity. This involves assessing possible risks, prioritising risks in terms of their possible impact on elections and developing mitigation measures taking this ranking of vulnerabilities into account. The Risk Management Matrix for Elections is a living document which will be regularly reviewed and discussed within the Network. It identifies the risks and possible mitigation strategies proposed by the Network for consideration by Member States within six categories: I) regulatory and institutional risks; II) informational and societal risks; III) physical risks; IV) cyber risks; V) operational risks; and VI) human risks. The table below provides a taxonomy of selected risks and mitigation strategies that are directly related to interference threats to critical election infrastructure.

Risks	Possible mitigation strategies
<b>Physical Risks</b>	
Unauthorised access to polling stations and counting centres and tampering with ballots and other voting and counting logistics	Robust security measures and secure storage of voting and counting materials, including tabulation protocols
Disruption of essential services, such as power, water or transport	Backup power and water supplies, and contingency plans in case of infrastructure failure
Barriers to accessing voting facilities and materials	Accessible polling stations and voting materials for voters with disabilities
<b>Cyber Risks</b>	
Hacking or tampering of voting and tabulation information systems	Robust security measures, including firewalls and intrusion detection systems Paper audit trail or distinct electronic audit trail Deploying capabilities to ensure continuity of activities in the event of an incident Logs, detection mechanisms and efficient network filtering

	<p>Improving system robustness to ensure the capacity to withstand an increase in the volume of requests (denial of service attacks)</p> <p>Comprehensive application of security updates on the components exposed on the internet</p> <p>Reporting incidents on the exposed information systems to the cybersecurity authority without delay</p>
Data breaches	Robust security measures, including encryption and secure storage of sensitive data
Cyber-attacks on the voting system or electoral infrastructure, including phishing or malware	<p>Increasing cybersecurity awareness</p> <p>Implementing robust security measures, including antivirus software and regular software updates</p> <p>Enhancing capabilities to ensure a continuity of activities in the event of an incident, including recovery capabilities</p> <p>Logs, detection mechanisms and efficient network filtering</p> <p>Improving system robustness to ensure the capacity to withstand an increase in the volume of requests (denial of service attacks)</p> <p>Comprehensive application of security updates on the components exposed on the internet</p> <p>Reporting incidents on the exposed information systems to the cybersecurity authority without delay</p>
<b>Operational Risks</b>	
Voting system malfunctioning	Robust quality control measures, including testing and independent certification of voting systems
Inaccurate or incomplete election results	Robust quality control measures, including manual recounts and verification of vote counts and tabulation
<b>Human Risks</b>	
Voter and/or candidate intimidation	<p>Robust measures to prevent voter and candidate intimidation, including</p> <ul style="list-style-type: none"> <li>• notification and complaints mechanisms</li> <li>• dissuasive penalties</li> <li>• voter education and awareness campaigns</li> </ul>
Illegal conduct (such as bribery, vote buying, trading in influence, misappropriation, illicit political party financing, non-compliance with silence periods etc.)	Prevention measures and dissuasive sanctions, codes of conduct, candidate education and awareness campaigns
Electoral officials' misconduct, including tampering with votes or manipulating results	Robust selection procedures and integrity criteria, ethical codes of conduct, ethical training and orientation and dissuasive sanctions

Measures against voter and candidate intimidation risks are part of the [European Democracy Shield](#). The Commission announced that it will publish a Recommendation and a guide of best practices on the safety of candidates and elected representatives. Regarding illegal conduct disrupting the electoral process, the Commission focused on illicit financing of political parties in the European Democracy Shield, noting: "Transparency and accountability of funding in politics, including campaign financing, are key to prevent interference and critical to ensure a level playing field among political parties and candidates and to maintain citizens' trust in the integrity and fairness of elections". The Commission aims to support common work with the Member States on the transparency and integrity of funding in politics.

The European Cooperation Network on Elections' [Election Integrity Checklist](#) offers a checklist of possible measures to protect electoral integrity and election-related infrastructure:

- accurately identifying the entities operating election-related infrastructure;
- promoting awareness and contingency planning to mitigate disruptions;
- regular risk assessments and stress tests, whereby results are shared with relevant authorities;
- pro-active enhancement of the protection of election-related infrastructures, including facilities, equipment, networks, systems;
- pro-active actions for preparedness for, responsiveness to and recovery from cybersecurity incidents;
- technology used in elections is designed, developed and produced to ensure a high level of cybersecurity;
- cooperation between election and cybersecurity authorities;
- increasing awareness on cyber hygiene of entities related to elections, such as political parties, candidates and election officials.

Several table-top exercises have been organised ahead of the 2024 EP elections to stress-test Member States' crisis plans and responses to potential cybersecurity incidents. One such example is the cybersecurity exercise [EU ELEx 23](#), organised by ENISA and its partners. It took place in the European Parliament on 21 November 2023.

To counter malicious interference by state-sponsored proxies specifically, the [Hybrid CoE](#) encourages states to apply a '4 S model' as a means of protection and to build deterrence against such actors. This '4 S model' builds on four strands: situation, self, solution and synchronisation. 'Situation' stands for situational awareness, whereby a state's awareness should go beyond understanding which foreign power uses which proxy, by further asking "Who/Which institution of state X is responsible for backing proxy Y against state Z". 'Self' stands for a clear understanding of the capabilities and goals of the deterring state, for instance, if the state pursues deterrence together with other allies or on its own. 'Solution' refers to the identification of response options and available strategies. 'Synchronisation' means the coordination of measures, such as attribution, diplomatic measures and prosecution of criminals.

### [Election infrastructure and cybersecurity legislation](#)

In the EU, [critical infrastructure](#) must be protected against cyber incidents. The Directive on measures for a high common level of cybersecurity across the Union of 14 December 2022 ([NIS2-Directive](#)) provides rules on high cybersecurity standards for 18 critical sectors across the EU. Under these rules, medium-sized and large entities in these sectors must manage cybersecurity risks appropriately. They must also notify relevant national authorities of significant incidents. These are defined as incidents that could cause significant disruption or damage. Member States had until 17 October 2024 to [transpose](#) the NIS2 Directive. Not all Member States have [transposed](#) the Directive into national law yet.

The NIS2-Directive includes several elements of digital infrastructure in its scope, for instance, data centre service providers, trust service providers and providers of public electronic communications networks. It also includes the category of “public administration”. However, election infrastructure is not explicitly mentioned as falling within the scope. With its [proposed targeted amendment](#) to the NIS2-Directive of 20 January 2026, the Commission intends to expand the list of sectors of high criticality. Under “digital infrastructure”, the Commission proposed adding providers of European Digital Identity Wallets, providers of European Business Wallets and operators of submarine data transmission infrastructure.

The [Cyber Resilience Act](#) (CRA) makes online voting more secure by introducing cybersecurity requirements for devices connected to the internet. Smartphones, laptops and many other products with digital elements fall under the CRA, requiring manufacturers to follow a ‘security by design’ approach. The CRA also requires manufacturers to handle vulnerabilities during the entire lifecycle of their products. The main CRA obligations will apply from 11 December 2027, with reporting requirements applying as of 11 September 2026.

The new Cybersecurity Reserve under the [Cyber Solidarity Act](#) can be deployed upon request by a Member State to support the mitigation of the impact of significant or large-scale cyber incidents. In short, the Reserve is a pool of trusted security service providers that can be mobilised quickly if needed.

On 20 January 2026, the Commission published its [New Cybersecurity Package](#) to further strengthen the EU’s cyber resilience and simplify compliance with cybersecurity rules. This package includes a proposal on the [revision of the Cybersecurity Act](#). This proposal aims to address security challenges relating to information and communication technology (ICT) supply chains in critical infrastructure, specifically in sectors of high criticality and other critical sectors (as defined in the Annex to the NIS2-Directive). It seeks to reduce risks arising from dependencies and foreign interference by introducing a ‘trusted ICT supply chain framework’. Under the proposal, following prior assessments and verifications, a third country may be designated as a country posing cybersecurity concerns to ICT supply chains. Among other things, high-risk suppliers would not be entitled to participate in public procurement procedures.

The proposed changes would also strengthen ENISA’s mandate. The Commission proposed that ENISA would facilitate EU-wide cooperation, issue early alerts on cyber incidents and enhance situational awareness. The agency would also operate as a single-entry point for incident reporting in the EU. The Commission proposal further aims to establish a helpdesk with ENISA, Europol and the national ‘computer security incident response teams’ (CSIRTs<sup>2</sup>). This helpdesk would help with ransomware response and recovery. These measures would also apply to all aspects of election infrastructure if election infrastructure were to be designated as a critical entity under the NIS2-Directive.

### Including election infrastructure in the Critical Entities Resilience Directive

The idea to classify election infrastructure as a critical entity in order to introduce institutionalised safeguards has recurred in recent years. In its [final report](#) of 15 May 2023, the ING2 special committee stressed “the utmost importance of protecting the security, resilience and reliability of the election infrastructure, including, among other things, IT systems, voting machines and equipment, election office networks and procedures, voter registration databases and storage facilities”. The ING2 special committee [reiterated](#) its recommendation to classify digital election infrastructures as critical entities.

The CER Directive aims at strengthening the resilience of ‘critical entities’ that provide services essential for the economy and society as a whole, ensuring they can withstand all types of hazards. The Annex of the Directive lists the different sectors, subsectors and categories of entities that fall within its scope. Public

---

<sup>2</sup> Under the NIS2 Directive, each Member State shall designate or establish one or more national CSIRTs, which are responsible for incident handling.

administration is listed as a sector, including entities at the central government level. The Directive excludes entities that carry out their activities in the areas of national security, public security, defence and law enforcement. Member States are obliged to identify their critical entities for the sectors and subsectors set out in the Annex to the Directive by 17 July 2026. Once identified as critical entities in their respective Member States, these entities must I) carry out risk assessments to identify risks that could disrupt their ability to provide essential services; II) take technical, security and organisational measures to enhance their resilience; and III) report significant disruptive incidents to national authorities. The [Delegated Regulation of 25 July 2023](#) establishes a detailed, non-exhaustive list of essential services. This list is used by Member States' competent authorities to conduct their risk assessments and identify critical entities. Election infrastructure, however, is not included in the Annex.

The inclusion of providers of election infrastructure as critical entities could lead to increased [EU-wide cooperation](#) in this field: The [Critical Entities Resilience Group](#) fosters cooperation between Member States, particularly on sharing information and good practices. Further, the Commission provides support for critical entities, including on cross-sectoral risks, best practices, methodologies, cross-border training and exercises to test the resilience of critical entities.

## European Democracy Shield on elections and election infrastructure

The [European Democracy Shield](#), published on 12 November 2025, aims to “empower, protect and promote strong and resilient democracies across the EU”. The flagship action of the European Democracy Shield will be the creation of a new European Centre for Democratic Resilience. This Centre should bring together Member States' expertise and resources in responding to hybrid threats, enhancing collective response capabilities. The Centre should serve as a link between existing structures and networks. During the EUDS special committee's [extraordinary meeting](#) on the Communication on 24 November 2025, Commissioner Michael McGrath outlined that the initiative is based on a whole-of-society approach. The European Democracy Shield consists of three pillars. The second pillar “strengthening democratic institutions, fair and free elections and free and independent media” includes the following initiatives on elections and election infrastructure:

- intensify support for Member States under the [European Cooperation Network on Elections](#) to enhance electoral integrity and preparedness;
- present guidance on the responsible use of AI in electoral processes;
- update the [Digital Services Act \(DSA\) Elections Toolkit](#);
- support the establishment of a voluntary EU network of influencers;
- support common work with the Member States on the transparency and integrity of funding in politics;
- publish a Recommendation and a guide to best practices on the safety of candidates and elected representatives;
- reinforce cooperation with international election observers to strengthen capacities to monitor disinformation on social media during election observation outside the EU.

### The European Democracy Shield

Pillar 1) Reinforcing situational awareness and supporting response capacity to safeguard the integrity of the information space

Pillar 2) Strengthening democratic institutions, fair and free elections, and free and independent media

Pillar 3) Boosting societal resilience and citizens' engagement

Source: [European Commission](#)

On [25 November 2025](#), Commissioner McGrath also presented these points in the plenary of the European Parliament. The Policy Department has published a [Briefing](#) "European Democracy Shield – Assessing the Commission's Communication" and a study "Strengthening resilience – Towards the European Democracy Shield" that were requested by the EUDS special committee. On 21 January 2026, the [draft report](#) outlining the findings and recommendations of the EUDS special committee was published. On 29 January, it was presented at an EUDS committee meeting. Voting on the report in Committee will take place on 23 June 2026.

## Weblinks

- European Commission, [Right to vote and to stand as a candidate at municipal elections](#), (2026).
- European Youth Portal, [EU Elections: different ways of voting across Europe](#), (2024).
- Service Public, [Peut-on voter par internet pour les élections politiques ?](#), (2026).
- NIS Cooperation Group, [Compendium on Elections Cybersecurity and Resilience](#), (2024).
- European Commission, [New Cybersecurity Package](#), (2026).
- European Commission, [Communication Securing free and fair European elections](#), (2018).
- European Commission, [Communication European Democracy Shield : Empowering Strong and Resilient Democracies](#), (2025).
- European Union Agency for Cybersecurity (ENISA), Ilias Bakatsis, [ENISA Sectoral Threat Landscape Public Administration](#), (2025).
- European Commission, [Memo: Known information interference operations during the June 2024 elections for the European Parliament](#), (2024).
- International IDEA, Jordi Barrat I Esteve, [Online Voting: Current and Future Practices](#), (2025).
- Republic of Estonia Information System Authority, ID website, [E-voting and e-elections](#), (2026).
- Council of Europe, [Guidelines on the implementation of the provisions of Recommendation CM/Rec\(2017\)5 on standards for e-voting](#), (2017).
- Valimised, [E-voting in other countries](#), (2026).
- National Institute for Research in Digital Science and Technology (INRIA), [The security of electronic voting: vulnerabilities and solutions](#), (2023).
- European Commission, [Compendium of e-voting and other ICT practices Non-Paper from the Commission services](#), (2023).
- International IDEA, [ICTs in Elections Database](#).
- European Parliamentary Research Service, [Digital technology in elections Efficiency versus credibility?](#), (2018).
- The European Centre for Excellence for Countering Hybrid Threats (Hybrid CoE), Sebastian Bay, [Countering hybrid threats to elections: From updating legislation to establishing collaboration networks](#), (2024).
- Reuters, [Polish police say three Warsaw polling stations had bomb alerts](#), (2023).
- European Cooperation Network on Elections, [A Risk Management Matrix for Elections](#), (2025).
- International IDEA, Sead Alihodžić, Erik Asplund, Ingrid Bicu and Julia Thalín, [Electoral Risks: Guide on External Risk Factors](#), (2024).

The European Centre for Excellence for Countering Hybrid Threats (Hybrid CoE), Janne Jokinen, Magnus Normark and Michael Fredholm, [Hybrid threats from non-state actors: A taxonomy](#), (2022).

The European Centre for Excellence for Countering Hybrid Threats (Hybrid CoE), Vladimir Rauta, [Countering state-sponsored proxies: Designing a robust policy](#), (2025).

European Union Agency for Cybersecurity (ENISA), [ENISA Threat Landscape for DoS Attacks](#), (2023).

The European Centre for Excellence for Countering Hybrid Threats (Hybrid CoE), Eginhard Volāns, Vladimir Rauta, Magda Long, Andis Kudors, Agata Kleczkowska and Eliza Lockhart, [Handbook on the role of non-state actors in Russian hybrid threats](#), (2025).

Forbidden Stories, ["Team Jorge": In the heart of a global disinformation machine](#), (2023).

The Guardian, [Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach](#), (2018).

Deutsche Welle, [Facebook data scandal: What you need to know](#), (2018).

European Cooperation Network on Elections, [Election integrity checklist](#), (2025).

European Union Agency for Cybersecurity (ENISA), [EU cybersecurity exercise: foster cooperation, secure free and fair EU elections](#), (2023).

European Commission, [Defending democratic values in the digital age](#), (2025).

European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 ([NIS 2 Directive](#)), (2022).

European Commission, [NIS2 Directive: securing network and information systems](#), (2026).

European Cyber Security Organisation, [NIS2 Directive Transposition Tracker](#), (2026).

European Union, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 ([Cyber Resilience Act](#)), (2024).

European Union, Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 ([Cyber Solidarity Act](#)), (2025).

European Commission, [Commission strengthens EU cybersecurity resilience and capabilities](#), (2026).

European Union, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 ([The Cybersecurity Act 2](#)), (2026).

European Parliament, [Report on foreign interference in all democratic processes in the European Union, including disinformation](#), (2023).

European Parliament, [Resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation](#), (2022).

European Parliament, [Draft report on the findings and recommendations of the Special Committee on the European Democracy Shield](#), (2025).

European Union, [Directive \(EU\) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC](#), (2022).

European Union, [Commission Delegated Regulation \(EU\) 2023/2450 of 25 July 2023 supplementing Directive \(EU\) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services](#), (2023).

European Commission, [Commission presents new best-practice election toolkit on the Digital Services Act](#), (2025).

European Parliament, Edoardo Bressanelli, [European Democracy Shield Assessing the Commission's Communication](#), (2025).

**Disclaimer and copyright.** The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2026.

Icon credits: © European Parliament

Administrator responsible: Olga Johanna PASSAMERA

Editorial assistant: Christina MARGELI

Contact: [poldep-just-b@europarl.europa.eu](mailto:poldep-just-b@europarl.europa.eu)

Print ISBN 978-92-848-3504-1 | doi: 10.2861/8755916 | QA-01-26-064-EN-C

PDF ISBN 978-92-848-3503-4 | doi: 10.2861/9047001 | QA-01-26-064-EN-N