**Study Guide**

**for the**

**Organization for Security and Co-operation in Europe**

**Topic Area:**

# Safeguarding Electoral Integrity in the OSCE Region: Addressing the Threat of Foreign Interference

## Table of Contents

# 1. Welcoming Letter

Distinguished Delegates,

It is with great pleasure that we welcome you to the Organization for Security and Co-operation in Europe (OSCE) at this year's RhodesMRC. We feel honored and excited to serve on the board of our committee. The topic of "Safeguarding Electoral Integrity in the OSCE Region: Addressing the Threat of Foreign Interference" is both urgent and complex, requiring a balance between national sovereignty, electoral transparency, and democratic values. Whether through disinformation campaigns, political funding, or diplomatic pressure, foreign actors have sought to sway electoral processes and undermine public trust in democratic institutions. We've reached a critical point, as recent developments have underscored the importance of the topic under discussion. Your role in this committee will be to develop strategies that strengthen electoral integrity while ensuring that OSCE values—transparency, fairness, and cooperation—remain at the heart of our efforts.

In this study guide, we aim to provide you with all the relevant background information necessary to understand the complexities of electoral interference. Additionally, we encourage you to conduct your own research, as a comprehensive grasp of this issue requires exploring multiple perspectives and case studies. The bibliography and further reading sections at the end of the guide will serve as valuable starting points for your investigation. On a special note, we kindly ask that you not only read this study guide carefully but also familiarize yourselves with the Rules of Procedure (RoP). On behalf of the Organizing Team and the Secretariat, we welcome you to RhodesMRC 2025.

We look forward to witnessing your insightful debates and diplomatic initiatives.

**Sotiris ANASTASOPOULOS**, *Chairperson-in-Office*

**Dimitra ANTONAROU,** *Secretary General*

# 2. Introduction to the Committee

## 2.1. History of the Committee[1]

The Organization for Security and Co-operation in Europe (OSCE) traces its origins to the détente period of the early 1970s, when the Conference on Security and Co-operation in Europe (CSCE) was established as a multilateral forum for dialogue between East and West. Following two years of negotiations in Helsinki and Geneva, the participating States signed the Helsinki Final Act on 1 August 1975. This landmark document outlined key commitments in the politico-military, economic, environmental, and human rights spheres, laying the foundation for what became known as the Helsinki Process.

Throughout the Cold War, the CSCE functioned primarily as a platform for diplomatic negotiations and periodic reviews of compliance with the Helsinki principles, however, with the fall of the Iron Curtain, the 1990 Paris Summit marked a turning point, transforming the CSCE into a more structured institution capable of addressing emerging security challenges in the post-Cold War era. The institutionalization process culminated in the 1994 Budapest Summit, where the CSCE was officially renamed the OSCE, reflecting its expanded role in promoting stability, democracy, and human rights.

Today, the OSCE is the world's largest regional security organization, encompassing 57 participating States from North America, Europe, and Asia. Its comprehensive approach to security addresses a broad spectrum of issues, from conflict prevention and arms control to good governance and human rights protection.[2]

## 2.2. Internal Bodies, Institutions, and Structures[3]

The Organization for Security and Co-operation in Europe (OSCE) operates through a network of internal bodies and institutions that support its mandate in promoting security,

[1] OSCE, "History," www.osce.org, n.d., https://www.osce.org/history.
[2] OSCE, "Who We Are | OSCE," Osce.org, 2018, https://www.osce.org/who-we-are.
[3] OSCE , "Institutions and Structures," www.osce.org, n.d., https://www.osce.org/institutions-and-structures.

democracy, and human rights across its 57 participating States. These bodies focus on conflict prevention, democratic development, media freedom, and dispute resolution.

**Decision-Making and Political Bodies**[4]

- **Summits** bring together Heads of State or Government of the OSCE participating States to set long-term priorities and provide strategic guidance for the Organization. These high-level meetings shape the OSCE's direction for years to come.
- The **Ministerial Council**, composed of the Ministers for Foreign Affairs of the participating States, serves as the OSCE's highest governing body at the ministerial level. It reviews ongoing work, adopts decisions, and ensures that the OSCE remains responsive to global and regional security challenges.
- The **Permanent Council** is the principal decision-making body that meets weekly in Vienna to oversee the day-to-day operational work of the OSCE. It implements the decisions taken at Summits and Ministerial Council meetings, providing a platform for continuous political dialogue among the participating States.
- The **Forum for Security Co-operation (FSC)** focuses on military security and stability in Europe. It plays a crucial role in implementing key confidence- and security-building measures, regulating military information exchanges, and ensuring democratic control over armed forces. The FSC also works on the non-proliferation of weapons of mass destruction and controlling the spread of illicit small arms and light weapons.

**Institutions and Supporting Bodies:**

OSCE Parliamentary Assembly: The OSCE Parliamentary Assembly (OSCE PA) consists of 323 parliamentarians from across North America, Europe, and Asia, serving as a forum for parliamentary diplomacy and debate. It plays a crucial role in election observation, conflict prevention, and the promotion of democratic institutions. Through its Annual Sessions, the Assembly provides policy recommendations to the governmental structures of the OSCE. Special Representatives address specific issues such as border cooperation, national minorities, and regional conflicts, while fact-finding missions and parliamentary field visits enhance transparency and accountability. The

[4] *ibid*

OSCE PA maintains close cooperation with other inter-parliamentary bodies, including the Parliamentary Assembly of the Council of Europe and the NATO Parliamentary Assembly. The International Secretariat of the OSCE PA is based in Copenhagen.

OSCE High Commissioner on National Minorities (HCNM): The High Commissioner on National Minorities is tasked with identifying and addressing ethnic tensions that could escalate into conflicts. The Commissioner's mandate involves both short-term conflict prevention and long-term structural solutions to inter-ethnic tensions. If a participating State fails to meet its political commitments or international norms, the High Commissioner provides analysis and recommendations to assist in resolving the situation. Additionally, the HCNM publishes thematic Recommendations and Guidelines based on best practices to help states address common challenges regarding national minorities.

OSCE Office for Democratic Institutions and Human Rights (ODIHR): The ODIHR, headquartered in Warsaw, serves as the OSCE's main institution for promoting democracy, human rights, and the rule of law. It provides expert advice to governments on electoral processes, legal reforms, and democratic governance. ODIHR is best known for its election observation missions, assessing whether elections in OSCE participating States meet democratic standards. The Office also conducts training programs for law enforcement, government officials, and civil society organizations, with the goal of upholding human rights and combating discrimination.

OSCE Representative on Freedom of the Media: The OSCE Representative on Freedom of the Media monitors media developments and supports freedom of expression across participating States. Key responsibilities include ensuring journalist safety, promoting media pluralism, advocating for decriminalization of defamation, and combating hate speech while protecting free speech. The Representative provides legal expertise on media regulation, supports Internet freedom, and assists in the transition to digital broadcasting. Annual regional media conferences bring together journalists, policymakers, and civil society to discuss media challenges. Through these efforts, the Representative upholds independent journalism and democratic values in the OSCE region.

Court of Conciliation and Arbitration: Located in Geneva, the Court of Conciliation and Arbitration offers a mechanism for the peaceful resolution of disputes between OSCE participating States. Established by the Convention on Conciliation and Arbitration within the OSCE, the Court allows any State party to initiate proceedings against another participating State unilaterally. If conciliation efforts fail, the involved parties may opt for arbitration, where a legally binding ruling is issued. This

system offers a structured and diplomatic mechanism for resolving conflicts within the OSCE framework.

OSCE Minsk Group: The OSCE Minsk Group leads the organization's efforts to resolve the Nagorno-Karabakh conflict. Established in 1992, it is co-chaired by France, Russia, and the United States. The Minsk Group facilitates diplomatic negotiations and conflict mediation between Armenia and Azerbaijan, aiming for a peaceful resolution through dialogue and confidence-building measures.

OSCE Secretariat: The OSCE Secretariat, based in Vienna, serves as the administrative and operational hub of the organization. Under the leadership of the Secretary General, it provides logistical, financial, and strategic support to all OSCE operations. Additionally, the Secretariat houses the OSCE Documentation Centre in Prague, which preserves historical records and publications.

Additionally, while not direct OSCE institutions, certain bodies are closely linked to the Organization:

**Open Skies Consultative Commission (OSCC):** The Commission oversees the implementation of the Open Skies Treaty, which allows unarmed aerial observation flights over the territories of its 33 signatories. The OSCC meets regularly in Vienna to address treaty-related technical issues.

**Joint Consultative Group (JCG)**: also based in Vienna, monitors compliance with the 1990 Treaty on Conventional Armed Forces in Europe, ensuring transparency and stability in military capabilities across participating States.

### 2.3. Partners for Co-operation[5]

Security in the OSCE area is interlinked with neighboring regions. To strengthen dialogue and cooperation, the OSCE maintains privileged relations with 11 Asian and Mediterranean Partners for Co-operation:

[5] OSCE , "Partners for Co-Operation," www.osce.org, n.d., https://www.osce.org/partners-for-cooperation.

- Asian Partners for Co-operation: Afghanistan, Australia, Japan, Republic of Korea, Thailand.
- Mediterranean Partners for Co-operation: Algeria, Egypt, Israel, Jordan, Morocco, Tunisia.

The OSCE Secretariat supports the OSCE Chairmanship and the Asian and Mediterranean Partners for Co-operation Groups, organizing conferences and coordinating technical assistance projects upon request.

### 2.4. Mandate, Functions, and Capacities of the Simulated Organ[6]

#### Mandate of the OSCE Ministerial Council

The OSCE Ministerial Council is the central decision-making and governing body of the Organization for Security and Co-operation in Europe (OSCE). It convenes annually in the country holding the OSCE Chairmanship and serves as a platform for Foreign Ministers of participating States to discuss key security issues, review the Organization's work, and adopt new decisions and declarations.

#### Functions and Limitations

- Defining Political Priorities:
    - Ministers deliver statements outlining their country's positions on OSCE matters and broader security developments.
    - The OSCE Chairperson-in-Office and top officials present reports on the Organization's activities over the past year.
- Decision-Making and Consensus Building:
    - Delegates negotiate Ministerial Decisions and Declarations, which:
        - Mandate new OSCE initiatives and policies.

[6] U.S. Mission OSCE, "The OSCE Ministerial Council," U.S. Mission to the OSCE, December 2, 2016, https://osce.usmission.gov/osce-ministerial-council/.

        - Set political standards that all OSCE States commit to uphold.
    - The OSCE operates on a consensus-based system, meaning that all 57 participating States must agree for a decision to be adopted.
- Diplomatic Engagement and Side Events:
    - Ministers and senior officials engage in bilateral and multilateral meetings.
    - Side events on specific security issues provide additional forums for dialogue.
    - Civil society representatives may present recommendations to the incoming OSCE Chairmanship.

**Capacity and Deliverables**

- Adoption of Declarations & Decisions: The Ministerial Council's agreements shape OSCE policies, with commitments that are politically binding for participating States.
- Guiding OSCE's Work: The Council's outcomes influence the Permanent Council and other OSCE bodies in implementing new initiatives.
- Strengthening Cooperation: The Ministerial Council promotes engagement with OSCE Partners for Cooperation, expanding dialogue beyond participating States.

Despite challenges in reaching unanimous agreements, the decisions taken at the Ministerial Council reinforce the OSCE's role in promoting security, stability, and human rights across its region.

## 3. Introduction to the Topic Area

Free and fair elections lie at the heart of democratic governance, creating a safe environment where voters choose their representatives. Over the past few decades, the rise of foreign interference within the OSCE region has underscored the pressing nature of the issue, which threatens national sovereignty, regional stability, and trust in democratic institutions. Adversaries have employed methods ranging from cyberattacks and influence operations to spreading disinformation through fake news campaigns, as well as covert funding and media manipulation, to influence political outcomes and undermine public confidence in democratic processes.

Elections are a core objective of the OSCE, as its broad mandate enables the promotion of democratic values, human rights, and the rule of law through monitoring electoral processes and providing all necessary means to member states in their pursuit of stability and the upholding of democracy. Nonetheless, the continuous transformation of the geopolitical landscape, with rising tensions and conflicting interests, has created the perfect conditions for foreign interference, even in areas that extend beyond the OSCE's traditional framework.

This issue is particularly relevant across the Organization's diverse geographical landscape. In an era marked by rapid technological advancements, addressing this pressing matter is crucial to sustaining collective democratic resilience. There have been numerous examples of such incidents, most notably the American elections in 2016 and 2020, as well as the elections in Georgia and Romania in 2024, which have proven that the credibility of democratic systems, the autonomy of electoral choices, and the broader security architecture of the OSCE region are at stake.

## 4. Glossary

**Foreign intervention:** Foreign interventions refer to actions taken by a country or group of countries to influence or interfere in the affairs of another nation, often through military, economic, or political means. These interventions can be driven by a range of ideologies and motivations, reflecting the beliefs and priorities of the intervening countries, which are often tied to broader political party ideologies that shape foreign policy decisions.[7]

**ICTs:** ICT (information and communications technology) is the infrastructure and components that enable modern computing. Among the goals of IC technologies, tools, and systems is to improve the way humans create, process, and share data or information with each other. Another is to help them improve their abilities in numerous areas, including business, education, medicine, real-world problem-solving, and even leisure activities related to sports, music, and movies. There is no universal definition of ICT because the technologies, devices, and even ideas related to ICT are constantly evolving. However, the term is generally accepted to mean all devices, networking components, and applications.[8]

**Disinformation:** Disinformation is false information that is deliberately intended to mislead, intentionally misstating the facts. It refers to intentional falsehoods spread as news stories or simulated documentary formats to advance political goals, as well as systematic disruptions of authoritative information flows due to strategic deceptions.[9]

**Propaganda:** Dissemination of information, facts, arguments, rumours, half-truths, or lies to influence public opinion. It is often conveyed through mass media. Propaganda is the more or less systematic effort to manipulate other people's beliefs, attitudes, or actions using symbols (words, gestures, banners, monuments, music, clothing, insignia, hairstyles, designs on coins and postage stamps, and so forth).[10]

---

[7] "Foreign Interventions - Vocab, Definition, and Must Know Facts | Fiveable," Fiveable.me, 2021, https://library.fiveable.me/key-terms/ap-gov/foreign-interventions.
[8] Mary Pratt and Rahul Awati, "What Is ICT (Information and Communications Technology)?," Tech Target, 2019, https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies.
[9] "What Do We Mean by Disinformation? | IFES - the International Foundation for Electoral Systems," Ifes.org, 2023, https://www.ifes.org/Election-Case-Law-Analysis-Series/Lessons-on-Disinformation-and-Election-Disputes/what-do-we-mean-disinformation.
[10] Bruce Lannes Smith, "Propaganda," in *Encyclopædia Britannica*, January 21, 2024, https://www.britannica.com/topic/propaganda.

**Information Warfare:** Information warfare is an operation conducted to gain an information advantage over an opponent. It consists of controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems, and disrupting the information flow. Information warfare, while not a new phenomenon, features innovative elements due to technological advancements, resulting in the faster and broader dissemination of information on a larger scale.[11]

**Fake news:** News that conveys or incorporates false, fabricated, or deliberately misleading information, or that is characterized as or accused of doing so. Fake news can refer to information that is false, or it can be used by individuals who disagree with and want to discredit the actual facts.[12]

**Generative AI:** Generative artificial intelligence, or GenAI, uses sophisticated algorithms to organize extensive, complex data sets into meaningful clusters of information in order to create new content, including text, images, and audio, in response to a query or prompt. GenAI typically does two things: First, it encodes a collection of existing information into a form (vector space) that maps data points based on the strength of their correlations (dependencies). Second, when prompted, it then generates (decodes) new content by finding the correct context within the existing dependencies in the vector space.[13]

**Deepfakes:** Any of various media, esp. a video, that has been digitally manipulated to replace one person's likeness convincingly with that of another, often used maliciously to show someone doing something that he or she did not do.[14]

**Cybercrime:** Cybercrime refers to criminal activity that involves a computer, digital device, or network. It can include hacking, identity theft, spreading viruses, and cyberattacks on government or corporate systems.[15]

---

[11] Defence Education Enhancement Programme , "MEDIA – (DIS)INFORMATION – SECURITY," NATO DEEP ADL Portal , n.d., https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.
[12] Craig McEwan, "LibGuides: Fake News: What Is Fake News?," libguides.exeter.ac.uk, n.d., https://libguides.exeter.ac.uk/fakenews.
[13] George Lawton, "What Is Generative AI? Everything You Need to Know," Enterprise AI (TechTarget, 2023), https://www.techtarget.com/searchenterpriseai/definition/generative-AI.
[14] Oxford English Dictionary, "Deepfake, N. Meanings, Etymology and More | Oxford English Dictionary," *Oed.com*, 2023, https://doi.org/10.1093//OED//7847968874.
[15] Michael Dennis, "Cybercrime | Definition, Statistics, & Examples," in *Encyclopædia Britannica*, February 20, 2019, https://www.britannica.com/topic/cybercrime.

**Transnational Organized Crime**: Transnational organized crime involves criminal groups that operate across national borders. These groups often engage in illegal activities like drug trafficking, money laundering, or human trafficking, and increasingly intersect with political or cyber operations.[16]

[16] United Nations, "What Is Transnational Organized Crime? | United Nations," United Nations, 2024, https://www.un.org/en/peace-and-security/transnational-crime.

# 5. Legal Framework

## a. Introduction

In the face of escalating foreign intervention, electoral integrity demands a robust legal response grounded in authority, ethics, and strict international obligations. Many levels of law support this reaction, including civil and political rights, cybersecurity cooperation, and instruments to inhibit international influence. The International Covenant on Civil and Political Rights (ICCPR) guarantees the right to political participation and free, fair, and legitimate elections. The Universal Declaration of Human Rights (UDHR) also promotes non-discrimination and inclusive political participation, focusing on threats posed by foreign involvement. Although not legally enforceable, the OSCE's Copenhagen Document promotes transparency, pluralism, and separation of state and party, setting a benchmark for election behavior. The following tools establish a consistent legal and institutional framework for OSCE member states, enabling them to resist foreign interference while enhancing democratic resilience, the rule of law, and human rights.

## b. Copenhagen Document

During the 1990 Conference on Security and Co-operation in Europe (CSCE), the Copenhagen Document was adopted, paving the way for the establishment of the Organisation for Security and Co-operation in Europe (OSCE). The Copenhagen Document is one of the most comprehensive guides to democracy, human rights, and fair elections since the end of the Cold War. It reflects a shared vision among Member States for the building of democratic societies founded on respect for individual freedom and the rule of law. Although it is not a legally binding document, the paper holds paramount importance, especially in relation to the OSCE’s role in election observation and human rights systems, as it is considered the cornerstone of the committee’s mandate.

The Copenhagen Document affirms that democratic values are fundamental to the realization of the inherent dignity and equal rights of all member states, and it promotes democracy by urging governments and public institutions to uphold the rule of law and submit to the oversight of electoral monitoring mechanisms. It refers to the separation

between government institutions and political parties, aiming to prevent the merging of party interests with state infrastructure and to safeguard political plurality and fair competition.

Furthermore, the Copenhagen Document stresses the need for “fair-play” in the context of political campaigns. An informed and fair political process depends on fair and non-discriminatory access to media. Those elected after having acquired the required majority of votes, in accordance with the provisions of national law and democratic values, must be inaugurated and allowed to complete their full term.

The aforementioned is particularly important in the spirit of fair elections and non-political interference. The electoral criteria serve as a benchmark for evaluating and combating external threats, including disinformation campaigns, cyberattacks, and media manipulation. By supporting these values, OSCE member states not only confirm their commitment to democratic values but also promote the protection of electoral processes from any undue influence.

### c. Universal Declaration on Human Rights

The UDHR was adopted by the United Nations General Assembly on December 10, 1948. Articles 2 and 21 of the Universal Declaration of Human Rights (UDHR) establish the principle of democratic governments and political involvement in the framework of electoral integrity.

- According to Article 2, all individuals are entitled to the rights and freedoms of the UDHR regardless of race, gender, language, religion, political opinion, national or social background, property, birth, or other status. It also emphasizes that one should not consider the political or international standing of their area. Article 2 underlines fair and non-discriminatory access.
- Equally important, Article 21 supports the notion that everyone has the right to participate in their country's government, either directly or through freely chosen representatives. It ensures fair access to public services and claims that governance is founded on popular will. Legally and morally, Article 21 supports democratic elections.

These articles pertain to OSCE and electoral integrity vis-à-vis foreign interference.

### d. International Covenant on Civil and Political Rights (ICCPR)

The ICCPR, adopted by the UN General Assembly in 1966 and ratified in 1976, forms the cornerstone of international human rights law. It protects many political and social rights that are necessary for democratic societies. Democratic integrity is mentioned in Article 25, which protects citizens' freedom to vote, participate in public affairs, and be elected in honest periodic elections.

Article 25 establishes the legal and moral framework for election integrity in the OSCE, with most members being primarily ICCPR parties. Free and fair elections ensure democratic involvement in both procedural and substantive matters. To uphold democracy, the rule of law, and the people's ability to participate in government, OSCE member states must strike a balance between their national and regional obligations and their ICCPR commitments. The ICCPR remains an essential part of the OSCE's electoral authority and protection of human rights, despite the increasing complexity of foreign interference.

To conclude, the ICCPR not only protects rights but also requires the member states to enforce them effectively. This means that governments must utilize legal, administrative, and technological tools to safeguard elections against excessive interference from external sources. The Covenant establishes a framework for addressing violations and provides a structure for states to follow when they identify threats to democratic integrity.

### e. UN Convention Against Transnational Organized Crime (UNTOC)

The UN Convention Against Transnational Organized Crime (UNTOC), established in 2000, provides a strong legal foundation for addressing international criminal activities that increasingly intersect with political and electoral systems. Although not specifically designed for election-related dangers, its clauses are especially pertinent given the evolving nature of foreign influence, which often involves transnational networks operating across cyber, financial, and political domains.

Foreign interference campaigns frequently depend on the infrastructure and strategies of organized criminal organizations. The Convention calls for state parties to prevent involvement in organized criminal groups, enhance mutual legal assistance, and increase cross-border investigative cooperation. When tracing the origins of electoral interference, often orchestrated abroad but executed through domestic proxies or covert financial channels, these legal instruments are proven invaluable.

Moreover, the Convention's emphasis on preserving democratic institutions and national sovereignty aligns closely with the OSCE's fundamental principles. Networks involved in money laundering, corruption, or cybercrime can indirectly but significantly endanger electoral integrity through their influence. As a result, the Convention can function as a fundamental legal instrument to support cooperative, transnational responses to politically motivated disruptions of electoral processes.

### f. Budapest Convention on Cybercrime (2001)

In 2001, the Council of Europe adopted the Budapest Convention on Cybercrime, the first internationally binding treaty dedicated to preventing offenses committed through the internet and computer networks. The Convention provides legal instruments and a framework for international collaboration that are crucial to the resilience of democracies in an era where foreign interference often takes the form of organized disinformation campaigns, cyberattacks on electoral infrastructure, or digital espionage.

The Convention's primary objective is to promote cross-border collaboration, enhance investigative techniques, and harmonize national laws in the fight against cybercrime. It covers a broad spectrum of crimes, including but not limited to illegal access, data and system manipulation, computer-related fraud, copyright infringement, and network security violations, all of which could be possible vectors for upsetting political processes. Apart from its formal framework, the Budapest Convention has developed into an active forum for operational cooperation. It enables direct contact and relationship-building among practitioners, including law enforcement, prosecutors, and cybercrime units, across its more than 60 signatory countries.

Within the OSCE region, where cyber-enabled foreign interference has emerged as one of the most significant threats to electoral integrity, the Budapest Convention serves both as a critical legal instrument and a strategic pillar of democratic resilience.

### g. Conclusion

To conclude, in order to address the increasing threat of foreign interference, OSCE must depend on a well-defined and coherent legal framework, in addition to political will. As interferences are starting to cross international borders and attempt to undermine electoral integrity, the significance of these frameworks has become ever more relevant. However, the issue of whether the provisions of the frameworks above are enforced and respected remains a question of whether OSCE member states are collectively committed to upholding democratic legitimacy through law.

# 6. Main discussion of the Topic

## 6.1. Methods of foreign intervention

There is growing concern worldwide regarding the threat posed to democratic and fair elections by foreign interference, which is increasingly occurring through information and communication technologies (ICTs) and social media. Elections in the last decade and even these past few months have fallen victim to operations by adversaries aiming to erode trust and mislead the public. While foreign interference operations may not be a new phenomenon, the emergence of digital platforms and Internet culture has increased their scale, nature, and reach, making them a risk even for mature democracies.

In terms of methods, foreign intervention can be implemented in various ways. The main distinction focuses on covert versus overt intervention, but this is not the only, or even the most important, distinction that can be made. The spread of information communication technology, particularly the Internet, has decreased the frequency of Cold War-style covert operations since the risk of exposure has risen significantly. Interventions today are less about hiding the facts than manipulating the public's interpretation of those facts.[17]

### *6.1.1. Cyber-enabled election interference*

Election processes are under threat due to the surge of ICTs that provide a fertile ground for potential adversaries. In cases of election interference, violating the target State's sovereignty is the most probable international law infringement. Foreign powers are able to disable vital computer systems, such as deleting key files and rendering vote-tallying systems inoperable. Furthermore, another method of interfering in elections is the practice of flooding an online server with data requests, causing massive overload and hindering its operability, commonly known as a distributed denial of service (DDoS) attack. Potential adversaries might gain access to sensitive networks or devices that have a direct impact on the voting outcome, which is also a consequence of relying on ICTs.

[17] Kofi Annan Foundation, "Safeguarding Democracy: Navigating the Complex Landscape of Foreign Interference in Elections," Kofi Annan Foundation, September 2023, https://www.kofiannanfoundation.org/news/foreign-interference-in-elections-how-to-define-it/.

The above can happen in the following four ways. First, the electoral roll may be altered so that voters will be removed from it. Second, adversaries may change or completely delete votes from systems reliant on ICTs, especially in cases where tele-voting is used. Third, the election outcome may be altered by compromising the vote-counting software. Lastly, spreading misinformation regarding the outcome of an election can cause unrest and confusion.

The nature of the electoral process, as well as the information ecosystem in target States, will ultimately determine whether cyber-enabled interference attempts have a significant impact on the pre-election period; thus, States differ in their susceptibility. Foreign cyber interference in elections and referendums, or even the perceived risk, will continue to grow as the world becomes increasingly digitalized.

### *6.1.2. Disinformation, Propaganda, Information Warfare and Influence Operations*

New technologies also enable foreign powers to conduct influence operations aimed at aligning the political views of the target population with their interests. Nowadays, debates of a political nature happen in cyberspace, allowing foreign actors to interfere and pursue their malicious interests. It has been proven that controlling the information available to voters can significantly impact the outcome of a vote, especially when the information carries a political message.

The internet, due to its unique characteristics, enables foreign actors to influence political happenings in other states by providing the general public with news stories, opinions, and other forms of communication.

One feature of the Internet is that it enables foreign powers to directly influence political discussions in other countries by publishing news stories, opinion pieces, and other forms of communication on websites and social media. Influence operations violate international law when involving prohibited forms of communication, such as subversive propaganda. Although influence operations can involve the dissemination of factual information, the primary concern is the spread of misinformation, also known as fake news. While the primary concern is the spread of misinformation by domestic actors, states have also

expressed concerns regarding foreign adversaries intentionally circulating fake news to harm democratic processes.

Although fake news isn't protected under the principle of non-intervention, there is no explicit ban on its dissemination. Thus, it can be described as harmful only in cases when it can be characterized as coercive. The formation of political will relies on access to accurate and reliable information, as well as the ability of the public and political leadership to engage in legitimate and informed deliberation before making decisions. Fake news disseminates false information to influence and alter public behavior. Additionally, disinformation campaigns also rely on fabricated content, but it is specifically aimed at weakening or even paralyzing the decision-making ability by fostering false beliefs. Disinformation is intentionally deceptive, much like lying. Still, it is usually driven by political motives and goals, which, in cases of foreign interference, align with the interests of the foreign actor. The paralysis mentioned above is induced by causing confusion regarding the actual facts and eroding trust in the democratic system's ability to deliver a sound policy. These campaigns often operate at two different levels of deception: misleading the public and employing "sock puppet" tactics, such as creating fake online personas.[18]

Disinformation and propaganda are not inherently cybertools, nor are they explicitly used in the digital realm. While these tactics are not new, the introduction of ICTs and the internet has contributed to their widespread use and success. During election periods, these methods are commonly employed by supporters of political parties associated with the far right or far left. A common practice involved simplifying complex stories by distorting the actual facts and the narrative, and promoting them with sensational, eye-catching headlines.[19]

[18] Steven Wheatley, "New Technologies: New Challenges for Democracy and International Law," *DUKE JOURNAL of COMPARATIVE & INTERNATIONAL LAW* 31 (2018): 161, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1570&context=djcil.
[19] Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich, "Cyber and Information Warfare in Elections in Europe," CSS Cyber Defense Project, n.d., https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-08.pdf.

### *6.1.3. Use of AI in Cyberattacks Targeting Elections*

As generative Artificial Intelligence (AI)-enabled capabilities become more widespread, election officials must grasp the effects of these capabilities on the security and integrity of electoral systems. While AI offers opportunities to improve efficiency and strengthen election security and administration, it also raises concerns about potential risks, since malicious actors, including foreign states and cybercriminals, can weaponize AI to fulfill their ambitions.[20] AI-driven attacks carry the potential to disrupt voting processes and compromise key parts of the election infrastructure. However, AI can concurrently serve as a defensive tool, creating a dynamic in which it is used for both offensive and defensive purposes.

Additionally, AI-enabled "data poisoning" involves inserting misleading data into training assets, which can undermine the performance of AI systems intended to safeguard electoral processes. Countries with weaker cybersecurity defenses are at higher risk. Where security measures are outdated, these states are more vulnerable to attacks consisting of data manipulation and targeting their voting systems.[21]

Generative Artificial Intelligence (GenAI) is capable of creating highly realistic images, videos, and text, making it challenging to distinguish between authentic and fabricated content. This also raises vital ethical and legal questions regarding the responsibility for the generated content and how accountability should be assigned.[22]

Deepfakes are one of many tools used to spread intentionally false information (also called disinformation) online. During elections, they can be used to mislead voters, including providing false details about the process or fabricating statements by candidates. Sometimes, those sharing deepfake content may do so unknowingly, without realizing their inauthenticity.[23]

---

[20] "Risk in Focus: Generative A.I. And the 2024 Election Cycle | CISA," www.cisa.gov, n.d., https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle.
[21] Shivani Shukla , "AI and Elections," Cyber Defense Magazine, February 27AD, https://www.cyberdefensemagazine.com/ai-and-elections/.
[22] "An Overview of the Impact of GenAI and Deepfakes on Global Electoral Processes," ISPI, n.d., https://www.ispionline.it/en/publication/an-overview-of-the-impact-of-genai-and-deepfakes-on-global-electoral-processes-167584.
[23] "Don't Fall for Deepfakes This Election.," Combating the deceptive use of AI in elections, n.d., https://news.microsoft.com/ai-deepfakes-elections/.

This tactic not only erodes trust in institutions and democratic values but also fosters doubt about the credibility of information. Malicious actors can exploit this environment to achieve their goals by labeling genuine media as fake, thereby shifting blame onto their opponents. As public awareness of GenAI content increases, this tactic proves even more effective, ultimately leading the public to disregard legitimate messages altogether.[24]

### *6.1.4. The Role of Social Media in Election Campaigns*

In recent years, the nature of elections has undergone a significant transformation due to the increasing presence of social media. On this platform, news, discourse, and election information are widely shared. Hence, social media are a vital tool, able to impact elections and their result. Social media are hosting all sorts of information. The interactive and communal nature of social media can be compelling for elections and campaigns. Voters often use these platforms to discuss their position and share their support.[25]

Voter behavior and public opinion are susceptible to being influenced by media coverage of candidates, as the media provides the public with information about them and the topics under discussion. One typical practice of election news that can impact voting behavior is “horse race” or “game frame” coverage, where the spotlight is on who is leading or trailing in the election race, based on polls, debates, and fundraising. This method, while easy to produce for media personnel, can create mistrust and cynicism among the public's opinion of the candidates, since this style of portraying them establishes the image of someone interested solely in winning rather than serving their purpose. There are many potential sources of “bias” in media coverage of elections. For example, news media might give a particular candidate more coverage than others or use a more critical tone when covering certain candidates. News coverage also might disproportionately focus on policy issues or campaign events that benefit one party or candidate more than the other. In some cases, the media’s efforts to maintain balance can create false equivalencies where two candidates’ missteps are treated equally, even if one behaves more egregiously than the other. All of these factors can influence voters’ perceptions of the candidates. The

[24] ibid
[25] Tony Hoff, “Pro and Con: Social Media and Elections,” Survey & Ballot Systems, November 12, 2014, https://www.surveyandballotsystems.com/blog/engagement/pro-con-social-media-elections/.

incentives of social media platforms, which are designed to maximize attention and engagement, also facilitate the spread of misinformation. Misleading content, especially when it contains a partisan element, is often highly effective at activating people's emotions and encouraging them to "like" or share the content. This both increases the spread of the original misleading content due to social media algorithms that boost the visibility of engaging posts and motivates people to post misleading content in the future, with the hopes of getting others to engage with it.[26]

## 6.2. Challenges in Addressing Foreign Interference in Elections: The OSCE Perspective

The Organization for Security and Co-operation in Europe (OSCE), committed to upholding the principles of democratic integrity, national sovereignty, and openness, is being gravely tested in its ability to make adequate responses to the growing complexity and variety of external factors affecting democratic electoral processes. The OSCE must navigate complex legal, technological, and societal landscapes to ensure election integrity while upholding fundamental democratic principles, despite having a solid normative framework based on political commitments such as the 1990 Copenhagen Document.[27]

### *6.2.1. Attribution and Response*

Foreign election interference management addresses several challenges, namely attribution and response. Attribution to electoral integrity can be defined as the process of establishing and claiming responsibility for interfering with an election, e.g., a compromise of voting devices or the dissemination of false information. Response refers to the act of a state or actor answering to so-called involvement from whatever source, sanctions and prosecution, penalizing fines, public humiliation, or diplomatic efforts.

[26] Mike Lucas, "How Media – Namely News, Ads and Social Posts – Can Shape an Election," Rutgers.edu (Rutgers University, October 1, 2024), https://www.rutgers.edu/news/how-media-namely-news-ads-and-social-posts-can-shape-election.
[27] OSCE/ODIHR. *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE.* Copenhagen, 1990. https://www.osce.org/odihr/elections/14304
OSCE/ODIHR, *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE* (Copenhagen: OSCE, 1990), https://www.osce.org/odihr/elections/14304.

Attribution can be especially problematic in the context of cyber-enabled foreign affairs because criminal actors often take steps to anonymize themselves. Anonymous servers or third-party proxy servers, for instance, may route cyber actions through multiple countries.[28] For example, the Russian-linked Internet Research Agency used disinformation campaigns via imposter American social media accounts to sway public opinion in the 2016 U.S. election, showing how foreign entities can be manipulated and camouflaged in a home environment.

Ultimately, although the OSCE is not a law enforcement body, it is crucial to address foreign intervention through norm-setting, observation, transparency, and cooperation. Its input helps to create a common knowledge among participating states of what constitutes interference and what appropriate reactions are within a democratic framework. The OSCE could enhance its integration of digital threats into election monitoring, support cooperation with cybersecurity organizations, and encourage member countries to establish joint systems for verifying and responding to electoral interference in a lawful and coordinated manner, thereby improving this function.

### *6.2.2. Striking a Balance Between Electoral Integrity and Democratic Principles*

Efforts to preserve electoral integrity in an age of foreign meddling collide with democratic values, creating a complicated policy paradox. States have a responsibility to protect their electoral procedures from misinformation, cyberattacks, and the potential involvement of AI. On the other hand, too forceful or poorly constructed responses could violate the fundamental democratic values of the free and fair elections.[29] This tension is especially significant within the OSCE framework, as member states are committed to preserving the integrity of democratic processes, as well as the civil and political rights outlined in the Copenhagen Document (1990).

The OSCE's priority is clear: democratic openness cannot be compromised for the sake of election security. The Copenhagen Document confirms the rights to free expression, access

[28] Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President* (New York: Oxford University Press, 2018).
[29] OSCE/ODIHR, *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE* (Copenhagen: OSCE, 1990), https://www.osce.org/odihr/elections/14304.

to information, and the creation of political parties. In light of the above, it is evident that OSCE member states must adopt a balanced, rights-respecting approach to election protection in response to this conflict. Instead of reacting with broad and generic legislation, governments may gradually choose a "baby steps" policy to support electoral integrity and enhance democratic legitimacy rather than undermine it.[30]

Ultimately, grounded in voluntary agreements and reciprocal responsibility, the OSCE approach offers a fair framework for governments to enhance their electoral resilience without compromising human rights or the rule of law. The difficulty lies not only in combating intervention but also in doing so in a manner that strengthens public confidence, protects civil rights, and prioritizes the basic principles of democratic government.

### *6.2.3. Public Trust and Voter Behavior Analysis*

#### a. Disinformation, Voter Perception, and the Erosion of Democratic Legitimacy

Public trust is the cornerstone of a democratic government. Within the commitments of the OSCE, as established in the Copenhagen Document (1990) and augmented by the International Covenant on Civil and Political Rights (ICCPR, Article 25), the safeguarding of open participation and the establishment of public confidence in electoral processes is not only a political aspiration but also a normative imperative.

The most insidious type of external interference does not involve hacking into systems or manipulating vote tallies, but instead consists in shaping perceptions and choreographing public conversation in a manner that encourages skepticism. Disinformation campaigns, particularly those amplified by social media algorithms, thrive in environments where trust is already eroding. They operate not only by spreading lies, but also by undermining the credibility of democratic institutions.

This effect was observed in the 2020 United States presidential election, in which, according to the ODIHR final report, "large-scale disinformation and unfounded allegations

[30] Timothy Snyder, *The Road to Unfreedom: Russia, Europe, America* (New York: Tim Duggan Books, 2018).

of electoral manipulation seriously undermined public confidence"[31] and contributed to an unprecedented level of political polarization and post-election violence. The “January 6th Capitol insurrection” is a prime example of the power of disinformation to influence voters and incite real-world violence, driven by false narratives of election legitimacy propagated by both foreign and domestic actors.

Among the most harmful strategies employed by external actors is the dissemination of targeted disinformation, in which specific ethnic, religious, or ideological communities are inundated with false or misleading information expressly designed to exploit their vulnerabilities or historical grievances. Within the OSCE area, such tactics have most significantly impacted minority groups, diaspora groups, and young voters, typically with the intent to suppress electoral participation or alter political loyalties.

The OSCE has also continued to advocate for a comprehensive approach that encompasses institutional transparency, media responsibility, and civic education. The Office for Democratic Institutions and Human Rights, for example, has advocated for reforms to enhance the independence of electoral commissions, increase transparency in campaign finance, and introduce clear rules governing political advertising on the internet. Apart from these legislative measures, media literacy campaigns, such as those which were tested in Estonia and Finland in collaboration with civil society organizations, can be effective in equipping the public to counter disinformation through critical assessment and fact-checking. Simply put, undoing the erosion of public faith precipitated by exogenous stresses involves more than merely transferring technological innovation to electoral systems; it consists of renewing an ethic of openness, accountability, and participatory interaction.

### b. The Four Pillars of Public Trust in Electoral Processes

“Public confidence in the electoral process is the cornerstone of democratic legitimacy. Without trust, even the most technically sound elections risk being discredited.”

[31]OSCE/ODIHR, *United States of America: General Elections, 3 November 2020. Final Report* (Warsaw: OSCE, 2021), https://www.osce.org/files/f/documents/7/7/477823_2.pdf.

*- Matteo Mecacci, Director of the OSCE Office for Democratic Institutions and Human Rights (ODIHR)*

There is no doubt that electoral integrity is based on public trust. The public trust rests on four interconnected pillars: delivery, engagement, familiarity, and integrity—each of which captures how citizens and stakeholders assess the legitimacy of electoral processes and institutions. For OSCE/ODIHR, undermining public confidence, driven by disinformation and political polarization, has been a common thread in recent election observation missions. Developing these pillars upwards is not merely a matter of sound governance but a normative obligation under the 1990 Copenhagen Document and Article 25 of the ICCPR, both of which enunciate the right to effective democratic participation.

1. Trust of delivery is the perception that the electoral management body may conduct elections credibly. Above all, particularly in view of increasing digitisation, resource-poorness by EMBs[32], mismanaged reform processes or seeming lack of preparation are among the factors deteriorating such a trust. Guarantees are required on part of the EMBs by ensuring technical preparation, adequate means of finance as well as professional capability.

2. Engagement's trust is based on openness, inclusiveness, and communication. It shows the EMB's capacity to interact with voters, civic society, and other stakeholders by means of open communication and information-sharing. This pillar is reciprocal: proactive involvement creates support and protects.

3. Trust of Familiarity arises from predictability and continuity. Sudden electoral reforms, especially technological ones, may create distrust. EMBs can sustain this pillar by introducing changes gradually, increasing transparency, and communicating clearly with the public to reduce fear of disruption.

4. Trust of integrity: This is based on the 'moral character' and apparent independence of the EMB. This item differs from the first three as its basis is more on independence, fairness, and transparency rather than performance. Even EMBs with capabilities will find it difficult to achieve trust in contexts with deficits in democracy.

[32] OSCE/ODIHR, *Freedom of Media in Elections and Counteracting Disinformation*.

Together, these four pillars form the foundation for durable public confidence in electoral processes. For OSCE participating States, strengthening each is vital not only for democratic legitimacy but for resilience against both domestic and foreign threats to electoral integrity.

## 6.3. Key Stakeholders

### *6.3.1. Germany*

Germany is part of the OSCE and the EU, known for keeping high standards in civic culture, institutional independence, and electoral processes. However, recent developments highlight Germany's increasing vulnerability to multifaceted threats, particularly in the context of overseas interference, local extremism, and the destabilization of digital social media spaces. These issues are threats that endanger people's trust and faith in the system, which lies at the heart of OSCE commitments to human issues and the documents signed in Copenhagen in 1990.

#### a. Populism and Distrust in Voting: The Case of the AfD

The success of the Alternative für Deutschland (AfD) is a case of right-wing populism in Europe which features anti-elite sentiments, Euroscepticism, and undermining of liberal democracy. In the view of political experts Cas Mudde and Cristóbal Rovira Kaltwasser, populist movements arise from the narrative framing a "corrupt elite" out to get the "pure people." Such narratives reduce trust in electoral management bodies (EMBs) as well as in the media which perform crucial functions defined by OSCE inter-election standards.

During the 2021 German Federal Election, the AfD leadership has been alleging post-2020 US-style systemic discrimination and fraud,[33] without any proof of irregularities. These allegations are harmful not only in the domestic context but also in the context of

[33]OSCE/ODIHR, *Germany: Bundestag Elections, 26 September 2021. Final Report* (Warsaw: OSCE, 2022), https://www.osce.org/odihr/elections/germany/510126.

foreign-sponsored campaigns aimed at deepening social divides. In areas like Saxony and Thuringia, which have been strongholds for the AfD, a growing number of poll consumers from non-mainstream media, which is correlated with lower trust in institutions.[34]

ODIHR reports for Germany have noted increasing cyber insecurity as a growing concern for election particularity in the governance of law and administration of justice, as well as breach of public order and under electoral conduct. The messaging approach, including the usage of encrypted messaging platforms like Telegram, has created parallel media systems where institutional delegitimization rhetoric runs wild.

### b. Disinformation and Platform Deregulation: The Role of X

The rebranding of Twitter as X by Elon Musk has radically transformed the content governance policies on the platform. In the name of "free speech absolutism,"[35] some of the previous safeguards against hate speech, election denial, and disinformation were removed or relegated. For Germany, where electoral mobilization is increasingly intersecting with online political discourse, this shift has both regulatory and democratic implications.

Germany's NetzDG legislation, mandating the removal of illicit content (such as Holocaust denial or incitement of violence) within 24 hours, has suffered compliance issues since X was taken over. In 2023, the German Federal Ministry of Justice launched an investigation into X's moderation failures[36], noting that it had not acted on hate-driven and election-related disinformation, some of which recycled Russian and far-right disinformation.

This poses theoretical questions regarding digital sovereignty and the tension between state regulatory authority and private platform governance. In line with Helberger's "platform power" model, we can see that platforms like X have in effect become quasi-public spaces[37] but operate outside of conventional democratic control. Where electoral debate is facilitated

[34]Snyder, *The Road to Unfreedom*. http://cd.bos.rs/online-citanka-novi-lideri--nove-mogucnosti-10/uploaded/Timothy%20Snyder%20-%20The%20Road%20to%20Unfreedom(2018).pdf
[35]Dorothy E. Denning, *Information Warfare and Security* (Boston: Addison-Wesley, 1999).https://www.proquest.com/docview/206656899?sourcetype=Scholarly%20Journals
[36]National Democratic Institute, *Disinformation and Electoral Integrity*.https://www.ndi.org/sites/default/files/Disinformation%20and%20Electoral%20Integrity_NDI_External_Updated%20May%202019%20%281%29.pdf
[37]Poznansky, “Deterrence and Foreign Election Intervention.”https://academic.oup.com/jogss/article/9/2/ogae011/7673991

by parties who are not interested in adhering to state regulation—or even who actively platform misinformation—the OSCE's underlying values of pluralism, fairness, and transparency are threatened.

### c. Foreign Influence and Strategic Narratives- the OSCE Impact

Germany is a frequent target of external influence campaigns, predominantly from Russia, as confirmed by Germany's internal intelligence service, the Bundesamt für Verfassungsschutz (BfV). These campaigns often align with populist narratives, including anti-EU sentiment, anti-immigrant rhetoric, and perceptions of Western institutional and moral decline. In the 2021 federal election campaign, state-funded media such as RT Deutsch propagated material[38] questioning COVID-19 measures, democratic legitimacy, and electoral integrity—narratives boosted by AfD outlets.

From a hybrid war perspective, this disinformation serves strategic ends: to weaken domestic unity, destabilize democratic legitimacy, and reduce confidence in transatlantic relationships. Authors Thomas Rid[39] and Ben Nimmo[40] have documented how foreign actors progress from hard propaganda to "narrative laundering", injecting falsehoods into local storytelling, often through extremist media and populist echo chambers.

From an OSCE perspective, these German trends challenge the normative goals articulated in the Copenhagen Document, specifically the principles of equal suffrage, fair access to the media, and confidence in electoral institutions. The erosion of public trust underscores the need for a comprehensive, multi-level response. Nevertheless, structural problems remain, most notably in the responsibility for real-time platforms, transparency in online campaigning by political parties, and maintaining civic confidence in the long term. As ODIHR firmly recommends, trust is not established through simple respect for the law, but through a constant commitment to openness, engagement, and ethical conduct.

[38]OSCE/ODIHR, *Germany: Bundestag Elections 2021*.

[39]Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

[40]Ben Nimmo, “Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age,” Atlantic Council, 2017, https://www.atlanticcouncil.org/in-depth-research-reports/report/weapons-of-mass-distraction/.

### *6.3.2 Georgia*

The 2024 elections in Georgia were characterized by political violence and irregularities, as reported by officials deployed nationwide by a joint OSCE, EP, CoE, and NATO task force. The official results posted by Georgia's Central Election Committee allocated 53% of the vote to the ruling party, Georgian Dream, and 38% to the opposition coalition.[41] The election was widely seen as a referendum on Georgia's future geopolitical direction. The country's Russia-friendly authorities sought to secure a mandate for a pro-Kremlin manifesto, while opponents aimed to return Georgia to its path of Euro-Atlantic integration.

The Georgian Dream party has been in power for 12 years and is committed to the country's pro-European integration. In recent years, however, key party members have become increasingly critical of Western policies, for many, an aftereffect of Russian influence. Most notably, in 2024, stricter laws were adopted, similar to those of the Kremlin. Georgian Dream had vowed to ban opposition parties and bar their MPs from taking up their seats if it received a significant enough majority. Opposition parties have moved to dismiss the result of the election amid widespread reports of ballot stuffing, vote buying, and intimidation. Russia has refrained from officially celebrating the election victory of its Georgian Dream allies. Instead, Moscow has accused the West of trying to "destabilize" Georgia with calls for an investigation into alleged violations.[42]

During the pre-election period, representatives of Western institutions repeatedly urged the Georgian government to withdraw the "transparency of foreign influence" law and other undemocratic legislation, and to ensure free and fair elections. Simultaneously, the Russian Foreign Intelligence Service issued several statements regarding the October elections, questioning the credibility of international election observation missions and expressing strong support for Georgian Dream. Furthermore, there have been longstanding reports of Russia funding various political forces and parties in Georgia, including the Alliance of Patriots of Georgia and members of the former Conservative Movement, who appear on its

[41] Gabriel Gavin and Dato Parulava, "Georgia Election Marred by Intimidation and Interference, Observers Warn," POLITICO, October 27, 2024, https://www.politico.eu/article/georgia-elections-marred-by-intimidation-and-interference-observers-warn/.
[42] Nicholas Chkhaidze, "Russia Emerges as the Real Winner of Georgia's Disputed Election," Atlantic Council, November 12, 2024, https://www.atlanticcouncil.org/blogs/ukrainealert/russia-emerges-as-the-real-winner-of-georgias-disputed-election/.

electoral list. Despite this, Georgian Dream has neither challenged nor taken any measures against Russian funding of these parties, allowing pro-Russian forces to participate in the elections and engage in violent activities and disinformation.

In its assessment of post-election developments and complaints, the ODIHR found that cases were not considered sufficiently, which limited the availability of legal remedies. The forcible suppression of protests and numerous arrests raised grave concerns about compliance with international commitments to freedom of peaceful assembly.[43]

Summing up, the elections in Georgie 2024 highlight the important role of legitimacy in electoral processes in creating a stable national and international environment. The credibility, its partnerships, and the European future of Georgia are heavily dependent on legitimate and free governance, since without them, nothing can be taken for granted about the future that lies ahead.[44]

### *6.3.3. Romania*

On 6 December 2024, in an unprecedented move, Romania's Constitutional Court annulled the results of the first round of its 24 November presidential election, citing evidence provided by intelligence agencies that the electoral process had been "compromised throughout its duration and across all stages".

The candidate in the spotlight is Călin Georgescu, who has been publicly expressing pro-Russian, nationalist, and even fascist and antisemitic narratives. He is directly challenging Romania's European and NATO objectives, policies in close proximity to those of the Kremlin. In the first round of elections, shockingly, he took first place, receiving almost 23%, while the opposition received 19%. In his campaign, Georgescu employed unconventional means of communication, such as TikTok and Telegram, disseminating fabricated information that misled and polarized the public. Notably, tens of thousands of online user accounts that had been deactivated since 2016 became active just weeks

[43] "Following Georgia's Elections, ODIHR Reiterates Concerns over Pressure on Voters and Independence of State Institutions and Calls for Concrete Action," Osce.org, 2024, https://www.osce.org/odihr/elections/584050.
[44] "Foreign Interference in the Elections: What Georgian Dream Overlooks," Ug.edu.ge, 2024, https://medialab.ug.edu.ge/en/research/foreign-interference-in-the-elections-what-georgian-dream-overlooks.

before the elections, spreading pro-Georgescu content. The data has shown a clear use of artificial tools, including bots and GenAI products. Preliminary investigations have also revealed signs of illicit funding streams linked to foreign actors, sparking further controversy.

The annulment of Romania's election highlights the shortcomings of measures in addressing threats of a hybrid nature. Democratic institutions are still unprepared to counter the complexities of the modern era, where hostile foreign and private actors exploit gaps in cybersecurity, social media, and public awareness. This illustrates the ever-growing difficulty that electoral bodies and judicial systems face when dealing with issues arising from technological disruption and foreign interference. The case of Romania also sets a precedent, as states worldwide will be more frequently tasked with dealing with cases of foreign manipulation, compromised information integrity, and digital interference in election processes in the years to come.[45]

### *6.3.4. Portugal*

Portugal is a democracy characterized by high procedural integrity, low political polarization, and strong institutional safeguards.[46] It automatically receives favorable ratings in OSCE/ODIHR observation missions for its elections, which are characterized by high levels of transparency, efficiency, and adherence to international standards.[47] However, in recent years, even Portugal has begun to face challenges to its democratic strength, most strikingly in terms of heightened digital disinformation, populist thinking, and growing public distrust towards mainstream institutions.[48]

While Portugal itself hasn't been compelled to contend with the scale of intensity of disinformation that states like Germany or the United States have, it's far from immune itself. Its case offers a compelling glimpse at how subtle "wear and tear" -rather than

[45] "The Romanian 2024 Election Annulment: Addressing Emerging Threats to Electoral Integrity | IFES - the International Foundation for Electoral Systems," Ifes.org, 2024, https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity.
[46] "International IDEA. (2024). *General Election, 10 March 2024*. https://www.idea.int/node/157698
[47] OSCE/ODIHR. (2025). *Portugal: Early Parliamentary Elections, 18 May 2025*. https://www.osce.org/files/f/documents/7/a/590042.pdf
[48] Euronews. (2025). *Misinformation buffets Portugal ahead of snap elections*. https://www.euronews.com/my-europe/2025/04/30/misinformation-buffets-portugal-ahead-of-snap-elections

outright collapse—can aggregate to gradually erode the four pillars of public confidence in elections: delivery, engagement, familiarity, and integrity, as OSCE-compliant democratic values define.

### a. Populism and the Rise of Chega

The emergence of the far-right party Chega ("Enough") marks the arrival of Portugal to the far-right populism paradigm in Europe, which has been a topic of study by scholars and political scientists such as Cas Mudde.[49] Chega capitalizes on the public's frustration with the political elite, fosters an environment friendly to immigration, and exploits the unhappiness with judicial institutions that emerged following the 2019 legislative elections[50].

Despite Chega not being a popular political factor compared to its established counterparts, this discursive strategy poses a new challenge to Portuguese democratism. It consistently raises allegations against the electoral body and the media for bias, questioning their independence, and utilizes social media as a means to circumvent conventional gatekeeping.[51]

These strategies are directly undermining the pillars of trust, integrity, and engagement. Although there are no severe signs of electoral manipulation in Portugal, the party's rhetoric tends to normalize skepticism toward democratic institutions, creating an environment that could undermine the public's confidence in the long term, particularly among disgruntled voters and young people.

### b. Disinformation and the Digital Information Environment

The online space in Portugal is relatively limited, but dominated by global platforms like Facebook, YouTube, and TikTok. The OSCE/ODIHR did not conduct full-fledged election

[49]Mudde, C. (2019). *The Far Right Today*. Polity Press.
[50]Wall Street Journal. (2024). *The Populist Right Rises in Portugal*. https://www.wsj.com/articles/the-populist-right-rises-in-portugal-chega-party-7bb54090
[51]Washington Post. (2024). *How the far right is using social media in Portugal*. https://www.washingtonpost.com/video/world/how-the-far-right-is-using-social-media-in-portugal/2024/03/08/126a320b-58ba-4fd7-bfd3-f1d0c6df5208_video.html

observation missions for the 2021 presidential election or the 2022 parliamentary election; however, it noted that both domestic and EU-level civil society monitors recorded a significant amount of disinformation, particularly regarding immigration, COVID-19 restrictions, and political corruption.

Portugal's idiosyncrasy is the borrowing of foreign frameworks, namely those of U.S. far-right politics and more general European nationalist movements.[52] Chega party leader André Ventura, for instance, expressly compared his party to Donald Trump's electoral campaigns, adopting identical slogans and framing strategies (e.g., "Portugal first," "fake news media"). Norris and Inglehart, in the book Cultural Backlash, refer to these practices as "transnational borrowing," a key instance of discursive globalization in which local actors adopt populist strategies from elsewhere.

### c. Civil Society Resilience and Foreign Influence

In comparison to Germany, Portugal has been more hesitant in regulating digitization, adopting a softer regulatory approach. The Portuguese National Election Commission (CNE) is transparent, though it possesses limited power to control online information, especially on encrypted or decentralized platforms.

Furthermore, civic society in Portugal has been politically aware and active. Fact-checking organizations like Polígrafo and Aos Fatos have emerged as the go-to sources of countering political disinformation.[53] The European Digital Media Observatory (EDMO) hub for Southern Europe, co-led by Portuguese institutions, has ensured that cross-border disinformation monitoring becomes a reality during election periods. However, without legislative support, such efforts are confronted with constraints. Their efficacy depends on the voluntary compliance of platforms and citizen participation, both of which might be discredited by populist delegitimization efforts. The roots of delivery trust and engagement

[52]The Guardian. (2024). *Portuguese far-right leader criticised over police shooting comments*. https://www.theguardian.com/world/2024/oct/28/portuguese-far-right-leader-andre-ventura-police-shooting-comments

[53]SpringerLink. (2025). *Disinformation Dynamics and Regulation in Portugal: Insights from a Comparative Perspective*. https://link.springer.com/article/10.1007/s10610-025-09617-0

trust are, therefore, susceptible to gradual erosion in a vastly unregulated online environment.

From the OSCE perspective, the danger lies not only in blatant foreign interference but also in a lack of preparedness. A lack of proactive intervention can lead to strategic complacency, reducing the level of institutional vigilance and delaying the introduction of preventive actions. In light of the OSCE's focus on preventive measures and early warning, Portugal should continue to view the integrity of elections as an active goal, rather than a passive one.

### *6.3.5. United States of America- A Case Study of American Elections 2020*

The United States is arguably one of the most contradictory election climates. It's a high-tech, one of the most decentralized, and legislatively healthy electoral systems in the world. The 2020 presidential election demonstrated the susceptibility of democratic legitimacy to mass-scale disinformation, partisan polarization, and declining public trust.[54] These cycles demonstrated that election integrity is not solely a function of institutional capacity and procedural integrity, but also of individuals' subjective experience of the legitimacy of the democratic process, an aspect that is much more challenging to achieve in the digital age.

#### a. The U.S. 2016 and 2020 elections

The OSCE, as established by the 1990 Copenhagen Document, maintains a comprehensive mandate to support democratic elections, particularly through its Office for Democratic Institutions and Human Rights (ODIHR), which provides impartial election observation, guidance on electoral reforms, and mechanisms to enhance democratic

[54]OSCE Office for Democratic Institutions and Human Rights. (2021). *United States 2020 General Elections: ODIHR Observation Mission Final Report*. Retrieved from https://www.osce.org/odihr/elections/usa/477829

resilience. This mandate has become increasingly vital in the face of foreign interference campaigns targeting electoral sovereignty within its member states.[55]

A salient example is the 2016 U.S. presidential election, where Russian state-sponsored actors conducted cyber intrusions and disseminated disinformation to undermine democratic institutions and manipulate public opinion (Office of the Director of National Intelligence, 2017). Though the U.S. does not formally undergo OSCE election monitoring, the case reverberated across the OSCE region, highlighting vulnerabilities shared by many democracies. These incidents have prompted introspection within the OSCE regarding its normative legitimacy and operational effectiveness, arguing for a recalibration of institutional responses to emergent hybrid threats. The OSCE has since broadened its electoral integrity framework to integrate cybersecurity assessments, promote transparency in political financing, and foster international cooperation against disinformation—a critical evolution aligned with its core mission to uphold democratic governance. These developments underscore that safeguarding electoral integrity in the OSCE region demands not only vigilance against external actors but also continuous institutional innovation and legal coherence across participating States.

The 2020 American election was hailed as a success. In the face of complications from the COVID-19 pandemic, including the unexpected surge in vote-by-mail, early voting, and logistical adjustments, the election was well-managed across jurisdictions. The Cybersecurity and Infrastructure Security Agency (CISA) called it "the most secure in American history,"[56] and OSCE/ODIHR observers commended it for transparency, professionalism, and voter accessibility.

These commitments were in opposition to the political speeches issued following the election. Former President Donald Trump and his supporters refused to acknowledge the electoral defeat, instead making accusations of election fraud, manipulation, and

[55]Krebs, C. (2020). *Testimony before U.S. Senate Homeland Security Committee*.https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Krebs-2020-12-16.pdf

[56]CISA. (2020). *Statement from Director Krebs: 2020 Elections Were the Most Secure in American History*.

https://www.cisa.gov/news-events/news/statement-cisa-director-krebs-security-and-resilience-2020-elections

cyberattacks.[57] Social media, ideologically oriented media, and a strategically controlled group of influencers and bots actively spread those misconceptions and manipulate the public trust. This misinformation not only weakened confidence in the decision but also led to the Capitol revolt on January 6, 2021, a significant breach in the peaceful transition of power.

ODIHR's ultimate assessment was that "widespread disinformation and unsubstantiated claims of electoral fraud severely undermined public confidence and led to political fragmentation."[58] Trust in elections also became extremely polarized by party: a 2021 Pew Research Center survey reported that 76% of Republicans viewed the election as fraudulent, with no credible evidence to back up such a view.[59]

The elections serve as a reminder that electoral legitimacy cannot be assured solely through robust legal frameworks or institutions. In the United States, these conditions have been increasingly challenged by a political culture that prioritizes narrative over evidence, as well as by digital ecosystems that increase outrage and obfuscate the truth.

### *6.3.6. Cambridge Analytica- Case Study*

#### a. Introduction

Cambridge Analytica, established in 2013 as a subsidiary of the UK-based SCL Group, was a data analytics company focused on political microtargeting. Through a psychological

[57]Pew Research Center. (2021). *Republicans Who Relied on Trump for News More Concerned About Election Fraud*.

https://www.pewresearch.org/short-reads/2021/01/11/republicans-who-relied-on-trump-for-news-more-concerned-than-other-republicans-about-election-fraud/

[58]ODIHR (OSCE). (2021). *ODIHR Final Elections Report on the United States of America*.

https://osce.usmission.gov/odihr-final-elections-report-on-the-united-states-of-america/

[59]Partisanship, Social Desirability, and Belief in Election Fraud. (2024). *Politics*, SAGE Journals.

https://journals.sagepub.com/doi/10.1177/14789299241270462

profiling app, it leveraged Facebook's data-sharing policies to obtain the personal details of almost 87 million users, primarily without their consent.[60]

The impact of Cambridge Analytica (CA) on digital democracy is one of the most critical turning points. In the early months of 2014, the firm, led by hedge fund billionaire Robert Mercer and operated by Steve Bannon,[61] began to scrape users' Facebook pages without user consent on a massive scale. Through an academic partnership with fraudulent intent, this process created voter psychographic profiles aimed at influencing political activity in crucial elections, such as the 2016 US presidential election and the Brexit referendum. Former CA employee Christopher Wylie later revealed that the company's deliberate plan was "to target their inner demons," exploiting self-reported data to profile users to serve them politically charged advertisements tailored to their voting behavior. Facebook, for whatever reason, decided to circumvent a breach of securities law regarding its users' data in 2015, marking an era of irresponsible delay in addressing civil accountability. Reduced to the stakes of geopolitical dominance, the renaming of Twitter to X late last year by Elon Musk[62] signifies a decade-long decline in civility. Cambridge Analytica's exposed manipulation of data around elections is now met with X's blatant disregard for user options without any other alternatives.

### b. Cambridge Analytica: Targeting Democracy Through Psychographic Profiling and the role of X

Through a third-party app, Cambridge Analytica deceptively acquired the information of over 87 million Facebook users during the 2016 U.S elections. During this period, this data was utilized to construct psychological voter profiles, which guided advanced targeted disinformation campaigns during critical events such as the Brexit referendum. These

[60] Cadwalladr & Graham-Harrison, *The Guardian* https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach

[61] Cadwalladr, *The Guardian*, "I Made Steve Bannon's Tool" https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

[62] TechCrunch, "X: A Complete Timeline" https://techcrunch.com/2024/06/05/elon-musk-twitter-everything-you-need-to-know

strategies circumvented the customary scrutiny associated with election campaigns and exploited a loophole in digital advertising for political purposes. Cambridge Analytica's microtargeting policies further intensified the pre-existing polarization[63] while undermining public trust, disguised as an attempt to personalize their services.

The most controversial aspect to emerge after Musk's acquisition of Twitter in 2022 was the shift in the management of the platform alongside its political economy of user data. Twitter had functioned as a real-time news aggregator and public forum for users to express their opinions. Nevertheless, once Musk took over the platform and rebranded it as "X" in 2023, he adopted a different approach. Now, the platform is part of a vertically integrated technology conglomerate that includes social media, finance, and AI, all in one. The turning point for this change was the privacy policy update in August 2023, which allowed the collection of sensitive personal data, such as biometric identifiers and employment information, under the pretext of improving user services and refining AI chatbots, like Grok.

This change denotes another step in the history of digital capitalism: increased convenience and connectivity in exchange for heightened surveillance[64]. Monetization of user engagement was prevalent long before X, starting with Google and Facebook's data-driven ad model and behavioral tracking. However, X is unique in how it overtly integrates surveillance, generative AI, and user content, which is transformed into unconsented training data and provides no meaningful opt-out mechanisms or granular consent; therefore, users are stripped of agency. Unlike earlier platforms that euphemistically framed such practices behind privacy settings, X provides an overt approach that removes pretense; however, it lacks detail in service agreements, which can be redefined at will, bounded by unaccountability.

The thorough historical and legal context shapes this case study. The Cambridge Analytica scandal in 2018 raised expectations, particularly regarding the GDPR in the European

[63] FTC case report https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter

[64] Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.

Union.[65] X's edited policies have already sparked scrutiny from Ireland and Germany's National Data Protection Authorities, who contest whether the outlined consent meets the "freely given, specific, informed, and unambiguous" standard outlined in GDPR Article 4(11). These investigations are not only legally oriented but also emblematic of the ongoing struggle between national regulatory sovereignty and transnational platform power, a challenge that has persisted since the late 2010s. Historically, X represents a post-Cambridge Analytica phase in digital surveillance—one in which the informational asymmetry between platforms and users has become structurally embedded rather than simply exploited. While CA's tactics operated in the shadows, X's model represents a codified, normalized form of behavioral exploitation, openly acknowledged in its public-facing policies yet often insulated from accountability by platform design, terms-of-service complexity, and market dominance.

### c. Implications for the OSCE Region

The OSCE's 1990 Copenhagen Document emphasizes the right to seek and receive information, as well as the integrity of electoral processes. The CA scandal and X's evolving data practices both threaten these norms. Their legacy raises urgent questions about platform accountability, electoral resilience, and the role of international institutions in safeguarding democratic infrastructure. The OSCE must advocate for stricter digital transparency, user data protection, and standardized AI governance across its participating States.

[65] European Union, *General Data Protection Regulation (GDPR) – Article 4: Definitions*, accessed May 9, 2025, https://gdpr-info.eu/art-4-gdpr/.

## 7. Conclusion

Electoral integrity is fundamental to democratic governance; however, electoral processes across the OSCE region have come under growing threat from foreign interference. The threats vary in form, ranging from cyberattacks and disinformation campaigns to other forms of hybrid interference aimed at destabilizing democratic institutions. The case studies of Germany, Georgia, Romania, and the USA highlight that such interference is tailored to exploit the political and institutional vulnerabilities of each country.

This phenomenon reveals structural and political weaknesses within OSCE member states. Many electoral systems are technologically outdated; meanwhile, existing legal frameworks usually fail to address modern forms of interference, mainly in the digital realm, where fake news and disinformation can spread rapidly. The unregulated use of social media, the rise of genAI platforms, and gaps in campaign financing laws have contributed to an environment where foreign actors can easily fulfill their malicious purposes.

In light of the above, the OSCE has to strengthen its collective response mechanisms while simultaneously promoting democratic processes in elections. During the committee's sessions, delegates should aim to argue about the definition of foreign interference in a manner consistent with OSCE commitments, distinguishing between international engagement and illegitimate manipulation. It is also crucial to evaluate the preparedness of member states to protect their electoral systems, with a focus on cybersecurity and media manipulation.

Moreover, the role of OSCE itself should be thoroughly examined. Delegates should consider how the organization can improve its monitoring, reporting, and early warning systems, and how it will assist member states through best practice sharing, technical support, and observation missions. Ultimately, the committee is likely to develop realistic, well-grounded proposals that address the complexity of modern foreign interference.

## 8. Points to be addressed

1. How does disinformation undermine public trust in democratic institutions before, during, and after elections?
2. In what ways have foreign state and non-state actors manipulated media ecosystems to influence political discourse and voter preferences within the OSCE region?
3. How has the use of AI and deep fakes changed the landscape of political manipulation, and how will member-states address them effectively?
4. To what degree does the financing of disinformation campaigns and social media advertising by foreign actors affect electoral processes, and how should OSCE member-states monitor these threats?
5. How can OSCE member-states improve methods of attributing foreign interference in elections while respecting due process and avoiding politically motivated accusations?
6. How can participating States protect electoral integrity from cyber and disinformation threats without infringing upon fundamental democratic rights, such as freedom of expression and freedom of the media?
7. What specific strategies can OSCE recommend to rebuild and reinforce public trust in electoral processes, especially among young voters and minority groups?
8. How can the OSCE strengthen early-warning mechanisms and preventive diplomacy to counter electoral interference before it impacts political stability?
9. Given the increasing deregulation of major social media platforms, how should OSCE states coordinate to ensure accountability for election-related disinformation while maintaining an open digital public sphere?
10. What can the OSCE do to assist participating States where populist movements delegitimize electoral institutions without credible evidence, potentially fueled by external influences?

11. Given the erosion of content moderation standards on platforms like X, how can states like Germany strike a balance between freedom of expression and their duty to prevent electoral manipulation?

12. How should OSCE member-states respond when electoral legitimacy is contested not by external actors, but by mainstream domestic leaders and parties?

13. Should the OSCE develop a standard cybersecurity protocol or framework for elections across member states, focusing on resilience, attribution sharing, and rapid response to cyber incidents?

14. What lessons can be drawn from notable cases of the past (e.g., Germany, Georgia, Romania, USA), and how should these incidents influence the next steps towards resolving the issue of foreign interference?

15. What steps can OSCE member-states take to enhance the cybersecurity of election infrastructure, and how can they collaborate on cybersecurity initiatives to prevent foreign interference?

16. What are the ethical and legal challenges in developing AI-driven tools to detect interference schemes, and how can a balance be struck with civil liberties?

# 9. Bibliography

## 9.1. Primary Sources

1. Defence Education Enhancement Programme. “MEDIA – (DIS)INFORMATION – SECURITY.” NATO DEEP ADL Portal, n.d. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.
2. NATO Review. “NATO Review - Algorithmic Invasions: How Information Warfare Threatens NATO’s Eastern Flank,” February 7, 2025. https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html.
3. OSCE. “History.” www.osce.org, n.d. https://www.osce.org/history.
4. OSCE. “Who We Are | OSCE.” Osce.org, 2018. https://www.osce.org/who-we-are.
5. Osce.org. “Following Georgia’s Elections, ODIHR Reiterates Concerns over Pressure on Voters and Independence of State Institutions and Calls for Concrete Action,” 2024. https://www.osce.org/odihr/elections/584050.
6. U.S. Mission OSCE. “The OSCE Ministerial Council.” U.S. Mission to the OSCE, December 2, 2016. https://osce.usmission.gov/osce-ministerial-council/.
7. United Nations, “What Is Transnational Organized Crime? | United Nations,” United Nations, 2024, https://www.un.org/en/peace-and-security/transnational-crime.
8. www.cisa.gov. “Risk in Focus: Generative A.I. And the 2024 Election Cycle | CISA,” n.d. https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle.
9. www.osce.org. “Institutions and Structures,” n.d. https://www.osce.org/institutions-and-structures.
10. www.osce.org. “Partners for Co-Operation,” n.d. https://www.osce.org/partners-for-cooperation.
11. OSCE/ODIHR, United States of America: General Elections, 3 November 2020. Final Report (Warsaw: OSCE, 2021), https://www.osce.org/files/f/documents/7/7/477823_2.pdf.

12. 3OSCE/ODIHR, Germany: Bundestag Elections, 26 September 2021. Final Report (Warsaw: OSCE, 2022), https://www.osce.org/odihr/elections/germany/510126.
13. OSCE Office for Democratic Institutions and Human Rights. (2021). United States 2020 General Elections: ODIHR Observation Mission Final Report. Retrieved from https://www.osce.org/odihr/elections/usa/477829
14. Krebs, C. (2020). Testimony before U.S. Senate Homeland Security Committee.https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Krebs-2020-12-16.pd
15. CISA. (2020). Statement from Director Krebs: 2020 Elections Were the Most Secure in American History. https://www.cisa.gov/news-events/news/statement-cisa-director-krebs-security-and-resilience-2020-elections
16. ODIHR (OSCE). (2021). ODIHR Final Elections Report on the United States of America. https://osce.usmission.gov/odihr-final-elections-report-on-the-united-states-of-america/

### 9.2. Secondary Sources

1. Combating the deceptive use of AI in elections. “Don’t Fall for Deepfakes This Election.,” n.d. https://news.microsoft.com/ai-deepfakes-elections/.
2. Michael Dennis, “Cybercrime | Definition, Statistics, & Examples,” in *Encyclopædia Britannica*, February 20, 2019, https://www.britannica.com/topic/cybercrime.
3. Fiveable.me. “Foreign Interventions - Vocab, Definition, and Must Know Facts | Fiveable,” 2021. https://library.fiveable.me/key-terms/ap-gov/foreign-interventions.
4. Ifes.org. “The Romanian 2024 Election Annulment: Addressing Emerging Threats to Electoral Integrity | IFES - the International Foundation for Electoral Systems,” 2024. https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity.
5. Ifes.org. “What Do We Mean by Disinformation? | IFES - the International Foundation for Electoral Systems,” 2023. https://www.ifes.org/Election-Case-Law-Analysis-Series/Lessons-on-Disinformation-and-Election-Disputes/what-do-we-mean-disinformation.

6. Kofi Annan Foundation, “Safeguarding Democracy: Navigating the Complex Landscape of Foreign Interference in Elections,” Kofi Annan Foundation, September 2023, https://www.kofiannanfoundation.org/news/foreign-interference-in-elections-how-to-define-it/
7. Partisanship, Social Desirability, and Belief in Election Fraud. (2024). Politics, SAGE Journals. https://journals.sagepub.com/doi/10.1177/14789299241270462
8. George Lawton, “What Is Generative AI? Everything You Need to Know,” Enterprise AI (TechTarget, 2023), https://www.techtarget.com/searchenterpriseai/definition/generative-AI. Mike Lucas, “How Media – Namely News, Ads and Social Posts – Can Shape an Election,” Rutgers.edu (Rutgers University, October 1, 2024), https://www.rutgers.edu/news/how-media-namely-news-ads-and-social-posts-can-shape-election.
9. McEwan, Craig. “LibGuides: Fake News: What Is Fake News?” libguides.exeter.ac.uk, n.d. https://libguides.exeter.ac.uk/fakenews.
10. Oxford English Dictionary. “Deepfake, N. Meanings, Etymology and More | Oxford English Dictionary.” *Oed.com*, 2023. https://doi.org/10.1093//OED//7847968874.
11. Mary Pratt and Rahul Awati, “What Is ICT (Information and Communications Technology)?,” Tech Target, 2019, https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies.
12. Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich. “Cyber and Information Warfare in Elections in Europe.” CSS Cyber Defense Project, n.d. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-08.pdf.
13. Shukla , Shivani . “AI and Elections.” Cyber Defense Magazine, February 27AD. https://www.cyberdefensemagazine.com/ai-and-elections/.
14. Smith, Bruce Lannes. “Propaganda.” In *Encyclopædia Britannica*, January 21, 2024. https://www.britannica.com/topic/propaganda.
15. Tony Hoff. “Pro and Con: Social Media and Elections.” Survey & Ballot Systems, November 12, 2014.

https://www.surveyandballotsystems.com/blog/engagement/pro-con-social-media-elections/

16. Wheatley, Steven. “New Technologies: New Challenges for Democracy and International Law.” *DUKE JOURNAL of COMPARATIVE & INTERNATIONAL LAW* 31 (2018): 161. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1570&context=djcil.
17. 5Dorothy E. Denning, Information Warfare and Security (Boston: Addison-Wesley, 1999).https://www.proquest.com/docview/206656899?sourcetype=Scholarly%20Journals
18. National Democratic Institute, Disinformation and Electoral Integrity.https://www.ndi.org/sites/default/files/Disinformation%20and%20Electoral%20Integrity_NDI_External _Updated%20May%202019%20%281%29.pdf
19. Poznansky, “Deterrence and Foreign Election Intervention.https://academic.oup.com/jogss/article/9/2/ogae011/7673991
20. Ben Nimmo, “Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age,” Atlantic Council, 2017, https://www.atlanticcouncil.org/in-depth-research-reports/report/weapons-of-mass-distraction/.
21. “International IDEA. (2024). General Election, 10 March 2024. https://www.idea.int/node/157698
22. OSCE/ODIHR. (2025). Portugal: Early Parliamentary Elections, 18 May 2025. https://www.osce.org/files/f/documents/7/a/590042.pdf

### 9.3. Legal Texts

1. OSCE/ODIHR. Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE. Copenhagen, 1990. https://www.osce.org/odihr/elections/14304

### 9.4. Books

1. Timothy Snyder, The Road to Unfreedom: Russia, Europe, America (New York: Tim Duggan Books, 2018)
2. Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (New York: Farrar, Straus and Giroux, 2020).
3. Mudde, C. (2019). The Far Right Today. Polity Press.

### 9.5. Articles

1. Chkhaidze, Nicholas. “Russia Emerges as the Real Winner of Georgia’s Disputed Election.” Atlantic Council, November 12, 2024. https://www.atlanticcouncil.org/blogs/ukrainealert/russia-emerges-as-the-real-winner-of-georgias-disputed-election/.
2. Gavin, Gabriel, and Dato Parulava. “Georgia Election Marred by Intimidation and Interference, Observers Warn.” POLITICO, October 27, 2024. https://www.politico.eu/article/georgia-elections-marred-by-intimidation-and-interference-observers-warn/.
3. Ug.edu.ge. “Foreign Interference in the Elections: What Georgian Dream Overlooks,” 2024. https://medialab.ug.edu.ge/en/research/foreign-interference-in-the-elections-what-georgian-dream-overlooks.
4. Euronews. (2025). Misinformation buffets Portugal ahead of snap elections. https://www.euronews.com/my-europe/2025/04/30/misinformation-buffets-portugal-ahead-of-snap-elections
5. Wall Street Journal. (2024). The Populist Right Rises in Portugal. https://www.wsj.com/articles/the-populist-right-rises-in-portugal-chega-party-7bb54090
6. Washington Post. (2024). How the far right is using social media in Portugal. https://www.washingtonpost.com/video/world/how-the-far-right-is-using-social-media-in-portugal/2024/03/08/1_26a320b-58ba-4fd7-bfd3-f1d0c6df5208_video.html

7. The Guardian. (2024). Portuguese far-right leader criticised over police shooting comments.https://www.theguardian.com/world/2024/oct/28/portuguese-far-right-leader-andre-ventura-police-shooting-co mments
8. SpringerLink. (2025). Disinformation Dynamics and Regulation in Portugal: Insights from a Comparative Perspective. https://link.springer.com/article/10.1007/s10610-025-09617-0
9. Pew Research Center. (2021). Republicans Who Relied on Trump for News More Concerned About Election Fraud. https://www.pewresearch.org/short-reads/2021/01/11/republicans-who-relied-on-trump-for-news-more-concern ed-than-other-republicans-about-election-fraud/