

ARP 63

Strengthening Swiss Democratic Resilience in the Digital Age

Researchers: Camille Serrano, Ekain Mendiola Ardanza, Fiona Dedei and Vincens Gruber

Dr. Claudia Seymour

Faculty Lead: Souhaïl Belhadj-Klaz

Word Count: 12.608

Geneva, 20 May 2026

Note on the use of Artificial Intelligence: In preparing this report, the authors used Claude, ChatGPT, and Grammarly as writing-support tools; all substantive content remains the authors' own work.

List of Abbreviations

AFD	Alternative for Germany
AI	Artificial Intelligence
ARCOM	Regulatory Authority for Audiovisual and Digital Communication
CDU	Christian Democratic Union of Germany
CSA	Conseil supérieur de l'audiovisuel
DSA	Digital Service Act
EEAS	European External Action Service
EU	European Union
FDPG	Free Democratic Party of Germany
FDPS	Free Democratic Party of Switzerland
FIMI	Foreign Information Manipulations and Interference
GAI	Generative Artificial Intelligence
MP	Members of Parliament
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
OECD	Organisation for Economic Co-operation and Development
OFCOM	Federal Office of Communications (Switzerland)

SGDSN	Secretariat-General for National Defence and Security (France)
SIMODS	Structural Indicators to Measure Online Disinformation Scientifically
SPD	Social Democratic Party of Germany
SVP	Swiss People's Party
TV	Television
UN	United Nations
US	United States of America

Executive Summary

This report was commissioned by GVA² Fondation pour Genève and démocratie.tech as part of the Applied Research Project of the Geneva Graduate Institute's Interdisciplinary Master Program of International and Development Studies. It examines how digital disinformation threatens Switzerland's democratic resilience and proposes concrete measures tailored to the Swiss context. Based on a qualitative and comparative analysis, the report assesses disinformation campaigns targeting elections in France and Germany and analyses convergent patterns in disinformation strategies, institutional responses, and legislative frameworks. Against this backdrop, the report puts forth key findings and recommendations for safeguarding measures for Switzerland to strengthen resilience against disinformation.

Main Findings:

- Synthetic identities and deepfake videos are the most prevalent forms of disinformation in Germany and France during electoral periods.
- Switzerland's direct democratic system creates frequent and predictable windows for foreign disinformation operations, particularly during referendums and federal elections.
- The Swiss institutional response is fragmented across the Federal Chancellery, the Federal Intelligence Service, and OFCOM, with no dedicated agency to coordinate and actively implement counter-disinformation efforts.
- Switzerland lacks measures implemented by France and Germany, including pre-election cybersecurity assistance for political parties and platform accountability mechanisms.

Recommendations:

- Establish a dedicated federal anti-disinformation and counter-FIMI agency, modelled on France's Viginum and adapted to Swiss federalism and neutrality.
- Provide pre-election IT security support to parties and candidates, mirroring the Federal Office for Information Security in Germany.
- Move the OFCOM draft into binding law: algorithmic transparency, fast-track injunctions, reporting duties.
- Convert the 2019 and 2023 ad hoc convenings between Federal Government Officials and Meta, Google, and ByteDance into a standing pre-election coordination protocol.
- Enable and strengthen civil-society pre-bunking capabilities.

Table of Contents

1. Introduction.....	6
2. Literature Review.....	8
2.1 Disinformation Definitions.....	8
2.2 Disinformation Architecture.....	10
2.3 Democratic Resilience.....	11
3. Methodology.....	12
3.1 Methodological Approach and Limitations.....	12
3.2 Research Question.....	13
3.3 Case Study Design following Yin.....	13
4. The New Technological Landscape.....	14
4.1 Artificial Intelligence as an Exponential Threat.....	14
4.2 Algorithm-Driven Platforms and Their Ungoverned Amplification Structure.....	16
4.3 A Changing Threat Horizon: Short-Term Emerging Risks.....	18
5. Case Studies.....	20
5.1 Germany's Fertile Ground for Disinformation.....	20
5.2 Targeted Smear Campaigning and Deep Fakes Dominate Electoral Periods.....	21
5.3 From Trusting the Public to a Coordinated Task Force.....	24
5.4 Disinformation Exploiting Crisis and Fear in France.....	25
5.5 From Data Hacking to Long-Term Manipulation Operations.....	26
5.6 A "Diplomacy of Combat" Approach.....	29
5.7 Cross-Case Findings: Germany and France.....	31
6. Swiss Landscape Analysis.....	33
6.1 Switzerland's Media Environment: Stable but not Exempt.....	33
6.2 When Democracy becomes a Vulnerability.....	34
6.3 Interference from Abroad: Switzerland as a Geopolitical Target.....	35
6.4 Domestic Threat Vectors.....	37
6.5 A Fragmented Shield: Switzerland's Counter-Disinformation Architecture.....	38
7. What Switzerland is Missing: Institutional and Civil-Society Recommendations.....	40
8. Conclusion.....	42
Bibliography.....	45

1. Introduction

Democratic institutions are facing unprecedented challenges in the digital age. Several factors, such as the rise of new AI-driven technologies, the dominance of social media platforms and the automation of content distribution systems, have transformed information environments in which political participation is practised. In this landscape, disinformation has emerged as one of the key threats to the integrity of democratic processes. The European Union identifies disinformation as a major factor undermining democratic processes and public trust in institutions (European Commission 2025). As digital technologies continue to evolve, the methods through which these harmful actions are created and amplified also advance rapidly. Institutional responses struggle to adapt to the speed of this evolution, making up-to-date, effective responses challenging.

An overview and analysis of the technologies used to create and disseminate disinformation in the digital sphere is key to understanding the dimension and shape of the threat. Recent advances in Generative Artificial Intelligence, algorithmic amplification and automated content distribution have widened the possibilities to produce and intentionally spread false or misleading content online (Romanishyn et al. 2025, 3). Understanding how these tools function is necessary to effectively assess the threats and implications of disinformation.

Switzerland is often regarded as a model for democratic stability and resilience, yet it is not immune to these rapidly evolving processes. Despite its distinctive political culture, shaped by a long-standing system of direct democracy and its high levels of institutional trust, it is also facing challenges regarding the state of its information environment (Federal Council 2024, 16). The political and institutional architecture of the country, characterised among other things by its linguistic diversity, continued referendums, or the prevalent role as a host to international organisations, sets the ground for specific vulnerabilities that distinguish the Swiss case from other neighbouring countries (2024, 14-15).

In light of these considerations, the report will ask the following research question: *What strategies can democratic institutions and civil society organisations implement to strengthen Switzerland's democratic resilience against digital disinformation campaigns?* To answer this question, this analysis employs comparative case studies of France and Germany, two

democratic states that share cultural, linguistic, and institutional elements with Switzerland, and examines cases in which disinformation has shaped the latest electoral processes. By analysing the different methods and mechanisms used, the produced narratives, and the governmental responses designed in both countries, the paper provides lessons and practices that could be applied in the Swiss context.

The report is structured as follows: The first part presents a literature review that establishes the conceptual framework upon which the report is carried out. It defines disinformation and situates democratic resilience in contemporary scholarly debate. The methodology section outlines the qualitative comparative approach used, following Robert Yin's multiple case study design (Yin 2014). A chapter later examines the technologies and mechanisms currently used to produce and disseminate disinformation in the digital sphere, and then turns to the German and French case studies. The last chapter maps Switzerland's information environments and evaluates existing countermeasures. The report concludes with a set of recommendations designed to strengthen the resilience of Swiss institutions and democratic processes in the digital age.

2. Literature Review

2.1 Disinformation Definitions

Conceptualisations of disinformation vary considerably across international actors and scholarship. Therefore, an extensive literature review of the definitions of disinformation is essential to address vulnerabilities concerning the contemporary digital ecosystem. Intergovernmental organisations emphasise the different facets of disinformation. For instance, the European Union (EU) frames disinformation as a threat endangering democratic processes, public trust in institutional bodies and economic stability, as it targets and exploits political and societal vulnerabilities (European Commission 2022; European Commission 2025). In contrast, NATO situates disinformation primarily as a security threat, highlighting its role in undermining political cohesion among member states (NATO 2025). While these perspectives differ in their definitional focus, both acknowledge the potential for multidimensional harm through the active dissemination of disinformation.

The Swiss government adopts an approach that draws on both EU and NATO frameworks and situational disinformation within Switzerland's institutional context of democracy and political neutrality. The Federal Council of Switzerland states that disinformation is deliberately created and spread to weaken social and political trust while simultaneously polarising public debate and the validity of media institutions (Security Policy Report 2021, 8). The Swiss definition emphasises its manipulative purpose and distinguishes it clearly from accidental misinformation (Federal Council 2024).

The definition of disinformation of the German government aligns closely with the Swiss definitional scope. The government states that disinformation encompasses two central aspects, namely the dissemination of the manipulated information and the intent behind its spread. Furthermore, the government ties its definition to the described objective of actors spreading disinformation. According to the government, the goal is to influence opinions to harm a person, a certain social group, an organisation or a country (Federal Government Germany 2026).

The French government defines disinformation as the “dissemination of inaccurate information with a view to mislead and cause harm” (Ministry of Armed Forces 2025). Referred to as “manipulation of information” by French law as of 2018, disinformation is

evaluated by three criteria: whether the content is intentionally misleading of fact, disseminated in a large-scale, deliberate, and automated manner, and whether the dissemination is likely to impact election integrity especially in view of an upcoming election (Guillaume 2019, 4; General Secretariat for National Defence and Security 2021). Institutionally, the French government also defines disinformation within the context of foreign interference whereby disinformation is characterized by “coordinated campaigns directed by a foreign entity or state, intention to destabilize state institutions, and deployment via algorithmic amplification” (French Interministerial Directorate for Public Transformation, 2026; General Secretariat for National Defence and Security 2025).

Scholarship offers a wide range of definitions and contextualisations. Kupiecki (2025) offers a narrow conceptualisation as strictly tied to its intentionality and falseness (2025, 57). Therefore, the scholar defines disinformation as false information intentionally disseminated by state or non-state actors with malicious intent during times of peace, crisis, or war (Kupiecki 2025, 57).

Arce (2024), expands the conceptual understanding and argues that disinformation may also involve the dissemination of authentic information through deceptive methods, such as covert channels or false identities. This view challenges definitions of disinformation that strictly equate it to falsehood. Further, Ha et al. (2021) focus on disinformation and fake news, illustrating how both terms have evolved. Unlike Kupiecki and Arce, the framework they present allows for truthful and false information to constitute disinformation depending on the creator's intention and the audience's ability to evaluate credibility. The authors highlight the role of media literacy and recipient cognition, emphasising that the potential for harm depends not only on the content but also on the capacity of audiences to recognise false information (Ha et al. 2021, 291-292). The focus lies on misinformation rather than disinformation, which may reflect the evolving academic shift in recent years. Clear conceptual distinctions, however, remain important. Wardle and Derakhshan (2017) refer to misinformation as information shared without intent to cause harm, whereas disinformation is intentionally produced and disseminated to deceive, manipulate or inflict harm (Wardle and Derakhshan 2017, 20). Scholarship defines the term "malinformation," which reflects the strategic use of truthful information to harm through mechanisms such as leaks or harassment (Wardle and Derakhshan 2017, 20). It becomes clear that Wardle & Derakhshan (2017) have categorised terminology according to intention, whereas Arce (2017) and Ha et al. (2021)

have used definitions that include multiple perspectives. The strictest definition seemed to be provided by Kupiecki (2025), who centres disinformation around intent and falsehood. In sum, the Swiss government's conceptualisation partly aligns with contemporary scholarly and international definitions that focus on intent, manipulation, and societal and political harm. Nonetheless, Switzerland's approach puts a large emphasis on protecting democratic institutions and neutrality.

2.2 Disinformation Architecture

Kupiecki et al. (2025) describe the mechanisms of contemporary disinformation being increasingly linked to the use of digital technologies aiming to facilitate both the production and dissemination of disinformation on a wide scale. According to the authors, disinformation targets the consumer's cognitive vulnerabilities by focusing on different aspects, such as emotionally charged content (2025, 73). It is essential to note that methods of disinformation are rapidly changing, due to the incessant advancement of technological tools, particularly AI and automated bot networks. Depending on the source, disinformation combines overt and covert tools, such as black, white, and grey propaganda¹, including subversive and false-flag operations to destabilise targets or institutions (2025, 149). Operational stages of dissemination methods include techniques such as “whataboutism”, “attacks”, “mockery”, “provocations”, “exhaustion”, and “denial” against opposing opinions (2025, 150-51). Methods may vary by actor and the goal of the operation.

Cull et al. (2017) describe methods behind contemporary external operations dependent on diffused and unregulated online networks aiming to circulate information to destabilise target populations. Alternatively, Wardle and Derakhshan (2017, 37) emphasise the multifaceted nature of disinformation messaging and its overlaying aims, such as content that provokes emotional responses, content that relies on visual communication, such as memes and videos or content that promotes strong narratives and is repeated consistently.

The “firehose of falsehoods” model developed by Paul and Matthews (2016) points out the importance of ‘high volume’, ‘multichannel’ content that is spread rapidly, continuously and repetitively, without a commitment to objective reality or narrative consistency. Moreover,

¹White propaganda derives from a known source. Grey propaganda stems from an unknown or completely anonymous source. Black propaganda is considered to be information from a source in which the intent is to deceive (Cull et. al 2017, 17).

Marwick and Lewis (2017) provide evidence on how internet subcultures and far-right groups have adapted strategies (2017, 20) to manipulate discourse on- and offline. For instance, trolls, white nationalists and conspiracy theorists with diverging ideologies converge on shared influence tactics that exploit algorithmic platform metrics and the economic pressures of news platforms to gain viewership. These tactics can lead to the spillover of fringe narratives into mainstream dialogues, aiming to destabilise conversations and polarise within democratic contexts (Marwick and Lewis 2017). Overall, the literature review shows that scholars acknowledge that contemporary disinformation is characterised by digitally based operations aiming to destabilise targets. This is executed by limiting the ability of target audiences to decipher reality from fiction.

2.3 Democratic Resilience

As this report is intended to offer recommendations to strengthen Swiss democratic resilience against disinformation campaigns, it is critical to define the scope of democratic resilience and its relation to disinformation. Merkel (2025) defines democratic resilience by centring a democracy's capacity to absorb external challenges and internal stressors. Further demonstrating democratic resilience means having the ability to adapt to changing conditions of democratic governance without damaging democracy's defining norms, functions, and institutions (Merkel 2025, 3-4). Merkel (2025) argues that resilience is characterised by the interaction within a system and how its structures, functions, and actors effectively respond to changing contexts of external crises (2025, 3-4).

Burnell and Calvert (1999) discuss the notions of democratic capacity to define resilience in accordance with democracy's durability. Burnell and Calvert (1999) assess the durability of democratic systems by how well democracies can mount resistance to threats and prevent regression or loss of democratic qualities and practices, mainly on a temporary or exceptional basis (1999, 4). While the adaptability of democratic systems is dependent upon elements like durability, ultimately, for Burnell and Calvert, the resilience of democracy is contingent upon attachments to democratic values and ideals despite hostilities and differences that may exist in society (1999, 4). Their position on democratic resilience, along with Vaccari and Chadwick's (2020) findings on meaningful public debates, a core pillar of democratic resilience, is negatively impacted by disinformation, specifically deepfakes and AI-based synthetic content, accurately displaying the danger of disinformation within democratic

institutions. Their findings demonstrate that these methods can create uncertainty among citizens and enable malicious actors to deflect accusations by claiming that “nothing can be proven and believed” (Vaccari and Chadwick 2020, 9), while content that aims to destabilise institutional authority seeks to sow confusion and distrust in democratic societies (Arcos et al. 2020, 64-69).

3. Methodology

3.1 Methodological Approach and Limitations

This report adopts a qualitative approach that integrates, assesses and analyses a range of sources, including primary and secondary sources as well as civic interventions. Drawing on a wide range of source materials, it offers multiple perspectives on disinformation and electoral interference. Due to the fast pace of technological progress and the lack of available quantitative data, the report utilises primary sources produced by governments, such as reports, briefs, and informational materials. By doing so, it enables the research to assess and transfer data and findings from the case studies chosen to the Swiss context.

Furthermore, the report uses secondary sources to compare and frame methods and strategies of disinformation and its dissemination. The research profits from expert insight and can therefore build on existing research. Expert approaches are leveraged and will aid in developing feasible countermeasures and safeguarding mechanisms against disinformation in Switzerland.

The report acknowledges certain limitations which include the speed at which disinformation methods and technological tools are advancing. The research focuses on the most common tool of disinformation, such as AI and automated bot networks. For the case studies of France and Germany, the two most recent elections were chosen. This includes the Federal elections in Germany in 2022 and 2025, and for France, the presidential elections in 2017 and 2022. It is worth mentioning that Germany’s government had put policies and systems in place to safeguard the election in 2017 from interference. Nonetheless, those were not taken over in the election that followed.

3.2 Research Question

In a context where disinformation through digital means has been used (Federal Council 2024) by various actors - local and international - to interfere with democratic participation in Switzerland, the report aims to answer the following research questions.

What strategies can civil society and democratic institutions implement to strengthen democratic resilience against digital disinformation campaigns and related manipulative practices?

Additionally, sub-research questions were developed to delve deeper into contemporary democratic contexts and how disinformation strategies are used to destabilise democratic institutions. The following questions were constructed.

How are disinformation strategies visible in contemporary democratic contexts, in the form of electoral interference?

What disinformation strategies are used?

What can we learn from civil society organisations?

What are public institutions and other relevant actors doing to counter disinformation in digital environments?

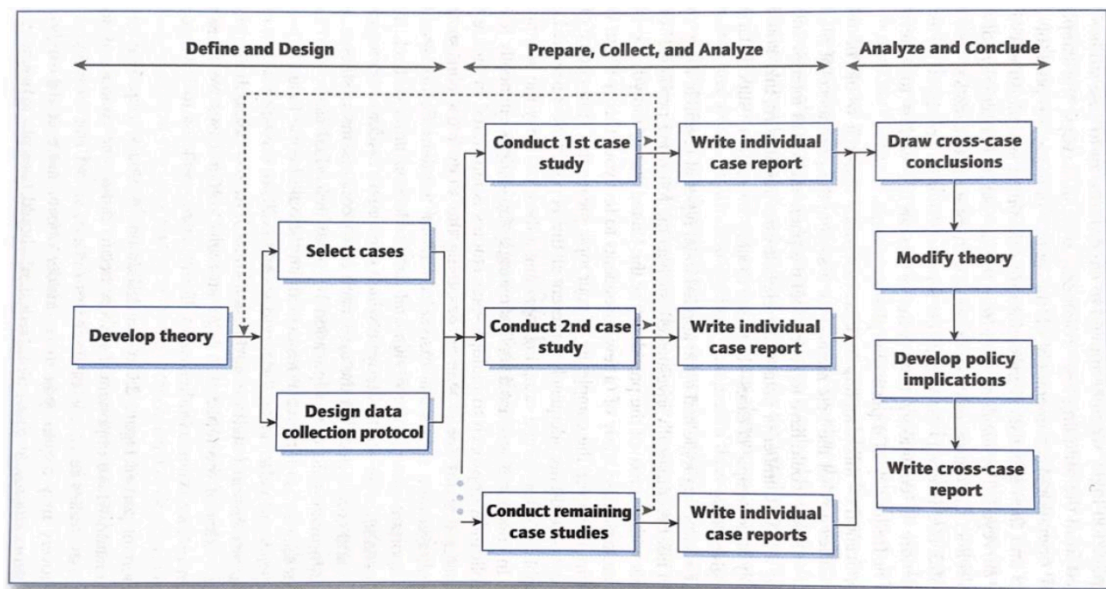
To answer these questions, two case studies, Germany and France, were evaluated, followed by a mapping of the Swiss information landscape, which includes an outline of Switzerland's trust in democracy and media as well as an analysis of statistical findings describing disinformation occurrences in the Swiss context. Further, safeguards, legal instruments and civil society participation are outlined to provide a foundation to the recommendations assessed for increasing Swiss resilience towards disinformation. By doing so, it provides a situational overview of Switzerland's digital vulnerabilities and enables comparisons with other countries to learn from and leverage best practices.

3.3 Case Study Design following Yin

In the context of disinformation during elections, France and Germany are used as the primary case studies for further analysis. Both countries share similarities with Switzerland due to language, institutional structures, and cultural norms. To methodologically analyse the

case studies, Robert Yin's case study design is applied, allowing for in-depth desk-based research of each country, to later identify patterns and differences in narratives and disinformation dissemination strategies. The methodological analysis process is depicted below.

Fig. 1: Case Study Procedure by Yin



(Yin 2014, 60).

The first step of Yin's multiple case procedure, as described above, entailed choosing the case studies. The second phase meant preparation, collection, and analysis of two elections in Germany and France. A contextualisation of the political and societal climate during the election time is described to understand disinformation methods used to destabilise the democratic process of fair elections. Individual case reports were written and summarised, followed by cross-case conclusions to identify common narratives, strategies and technological tools. These conclusions serve as the basis for producing effective research-based recommendations for Switzerland to combat disinformation.

4. The New Technological Landscape

4.1 Artificial Intelligence as an Exponential Threat

AI-generated disinformation differs from traditional human-generated disinformation in four potentially differentiating factors: scale, speed, ease of use and personalisation (Feuerriegel et al.). AI techniques to boost disinformation can be explained to come into play in two ways: First, AI generates new opportunities to create or manipulate texts and images, audio or video content. Second, AI systems developed by online platforms are highly efficient and contribute to the dissemination of disinformation online (Bontridder and Pouillet 2021, 3).

Generative Artificial Intelligence (GAI) systems enable low-cost, scalable content production and targeting, and the rapid expansion of social media has substantially increased the surface vulnerable to AI-driven disinformation campaigns (Romanishyn et al. 2025, 3). When GAI technologies are used to create fake content, the product is called a “deepfake” (Bontridder and Pouillet 2021, 3). This technology can be applied to various types of content, such as images, moving images, sound, and text. The term “deepfake” is primarily used for content in video or audio format.

These means of creating disinformation not only fuel the spread of false information, but also contribute to undermining the credibility of legitimate information, as they create doubts about any information encountered, even when it is delivered by the traditional press or by governmental administrations. These mechanisms, therefore, make it possible for anyone willing to mislead individuals to manipulate the truth in two effective ways: fake content passing off as authentic information, and authentic information passing off as fake (Bontridder and Pouillet 2021, 3).

Deepfakes are among the most widely used means of spreading disinformation; other means, such as bots and synthetic personas, are also widely used and operate across different scales (Romanishyn et al. 2025, 3). As for the dissemination, several methods have evolved in recent years, together with the expansion of AI tools: Microtargeting techniques and the web's advertising-driven economic model have fostered the development of AI-enabled tracking methods that lead platforms to precisely target users. These include methods such as fingerprinting, which relies on browser and operating system-specific characteristics to track users across websites (Bontridder and Pouillet 2021, 4).

Bots, as we commonly refer to them, respond to the definition of synthetic identities. These are fake personas generated with AI to appear as real people online; they commonly feature synthetic images along with fabricated names and personal details. Networks of such “personas” are then used to amplify false narratives, infiltrate groups, or lend false credibility to disinformation by posting as “concerned citizens” or experts (Romanishyn et al. 2025, 14).

The effect they achieve is that they can appear as many voices, creating the illusion of a broad consensus or grassroots support, infiltrate and even impersonate trusted individuals (2025, 15). AI has enabled bots to be far more sophisticated and effective agents of disinformation. Modern AI-driven bots can generate seemingly original content, engage in conversations, and operate within coordinated networks that ultimately amplify false narratives.

Fig. 2: Trends in the Context of Global Digital Dynamics (2019–2025)

Trend category	Observed growth	Benchmark insight	Relevance & interpretation
Deepfakes	5 × increase in deepfake content; +2,137% fraud attempts in North America	550% growth in global deepfake videos (2019–2023); 6.5% of all fraud in 2023 involved deepfakes	Mirrors an exponential content surge. Fraudulent deepfakes have shifted from niche uses (e.g., non-consensual porn) to mainstream scams and political impersonations, fueling nearly 40% of high-value fraud cases in 2024. Highlights a growing cross-sector risk, calling for stronger detection and legal safeguards.
Text generation	AI-generated news outpaced detection; fooled >50% of human evaluators	10 × increase in AI-generated fake news sites; 1,200 + sites by 2024; false news 70% more likely to spread than true	Illustrates rapid scale-up in misinformation production. Virality benchmarks show systemic threat to information integrity.
Synthetic identities	12.8 M + fake personas used for influence ops	\$35B in synthetic ID fraud losses; 5 × rise in forged identities; 1.3B + fake accounts disabled quarterly by Meta	Highlights ease of creating believable AI personas and difficulty in platform-level filtering. Economic cost shows systemic vulnerability.
Bots (automation)	~25% of Twitter activity was bot-driven	50% of total web traffic by bots (2023); ~30–37% from “bad bots”	Confirms that bot-driven amplification is widespread and not platform-specific. Confounds detection, skews public discourse.
Microtargeting	AI-enhanced propaganda reached ~34% of users	75% of firms use AI targeting; 3 × higher conversion for personalized ads; \$366B digital ad market	Personalized messaging has become default. Political targeting mimics commercial tactics – raises risks of manipulation and democratic erosion.
Real-time disinformation	Fact-check latency shrank from 45 to 15 min	Viral false news spreads ~6 × faster than truth; initial exposure shapes long-term belief	Even 15 min is enough to embed false narratives. Detection speed must be paired with pre-bunking and real-time mitigation tools.

(Romanyshyn et al. 2025, 4).

4.2 Algorithm-Driven Platforms and Their Ungoverned Amplification Structure

Platforms such as Facebook, X (formerly Twitter), Instagram, TikTok, YouTube, and Twitch have evolved from secondary distribution tools into infrastructural elements of contemporary journalism. Most of these platforms have changed the way in which information is consumed through algorithmic curation. These systems prioritise content based on passive or impulsive behaviours such as clicks, likes and watch time, which has reshaped what is counted as “news”. In this environment, newsworthiness is redefined as shareworthiness, incentivising content that elicits emotional responses and drives virality (Hastuti et al. 2025, 2).

Meta’s platforms, for example, including Facebook and Instagram, heavily rely on social network structures to curate and rank content in users’ feeds. They are structured upon algorithms that amplify moral-emotional content through social reinforcement mechanisms (Scharfbillig et al. 2026, 20). This growing reliance on algorithmic personalisation raises concerns about the emergence of “filter bubbles”, in which individuals become intellectually isolated due to fully automated recommendation systems (Baumann et al. 2026, 2).

According to a report by the SIMODS project (Science feedback 2025), disinformation is widespread through major platforms. TikTok shows the highest prevalence at approximately 25% of exposure-weighted posts, followed by Facebook (15%) and YouTube (12%). Platforms provide fertile ground for AI-generated disinformation. On video platforms such as TikTok, as of the time of the report, AI-generated content accounted for approximately one quarter of all identified disinformation. Among this content, only 16% is visibly marked as synthetic, demonstrating a failure of platforms to inform users of what they are consuming. The report shows that on X/Twitter, an account posting false or misleading information receives around 10 times as much engagement per post as a credible source. This becomes relevant taking into account that among younger generations, 44% of 18–24s declare that social media is their main source of news and 38% for 25–34s" (Newman et al. 2025, 14)

There is a concern that by prioritising engagement, content might amplify what is attention-grabbing but misaligned with user values or broader societal values (Milli et al. 2025, 1). Brady et al. (2023) introduce the concept of “prime” content, which algorithms tend to amplify, and define it as emotional, moral, prestigious, and in-group-oriented. This amplification has several consequences for the disinformation landscape: It contributes to an

out-group hostility, as users are frequently exposed to content that makes them feel worse about their political out-group and better about their in-group. This phenomenon is well-known as the echo chambers, defined as conflicting camps creating and reinforcing opposing identities (Scharfbillig et al. 2026, 21). Platforms use personalised rankings to show content by other users who have a like-minded online behaviour, which further contributes to increasing polarisation (Germano et al. 2025, 3).

Moreover, the predominant algorithmic logic of platforms prizes emotional intensity and prioritises negative emotions such as anger, sadness, or anxiety. Anger is the predominant feeling amplified by the engagement-based rankings (Milli et al. 2025, 5). Germano et al. (2025, 33) suggest that the design of digital platforms entails a tension between maximising engagement and preserving a healthy information environment.

Large Language Models, such as OpenAI's ChatGPT, have been labelled as "manipulation machines" (Simchon et al. 2024, 3). These models use AI to generate personalised political messages that target individuals based on their psychological vulnerabilities. Automated personalisation by means of generative AI enables the creation of personalised versions of a political message from a single template, tailoring the tone to the specific public based on different personality traits.

While the effect on personalised ads may be small, the effects become substantial at scale. A study revealed that out of every 100,000 individuals exposed to political messages tailored to their personality, 2,490 individuals would be expected to be persuaded due to the style. As they put it, considering that elections are often decided by fractions of a percentage point, shifting a few thousand individuals out of 100,000 can influence relevant political outcomes significantly (Simchon et al. 2024, 3).

4.3 A Changing Threat Horizon: Short-Term Emerging Risks

The growing use of generative AI and disinformation strategies, together with the ad-hoc landscape that social media platforms provide, means these technologies have the capacity to shape narratives and influence opinions. One of the main consequences of the prevalence of these mechanisms is the erosion of citizens' trust in information, public institutions and the

media. Moreover, it negatively impacts the right to participate in public debate (Bontcheva et al. 2024, 23).

Citizens need to have access to diversified information in order to form their own opinion, nevertheless, the digital ecosystem presents constraints to the ability that individuals have to make free and informed decisions. Through means of effective manipulation of opinions and the influence that this can have in voting decisions, the capacity to participate in the democratic discourse is impaired. (Bontridder and Pouillet 2021, 6)

In this same line, the concept introduced by Hastuti et al. (2025) “Shareworthiness”, helps us consider the reconfiguration of journalistic legitimacy, as social media platforms now function as infrastructural elements that prioritise sensationalism over professional editorial judgment (Hastuti et al. 2025, 1). Due to how platforms are structured nowadays, cognitive effort is reduced, fostering ideological segregation. Even though information is overabundant, attention leads to concentrate on a limited set of sources, which leads to a reduction in the diversity of information intake (Scharfbillig et al. 2026, 21).

GAI, as the predominant innovative technology, enables the creation of entirely artificial information environments that may, in the near future, be hard to evaluate as such. Not just fake images or text, but interconnected systems in which the content, the people sharing it, and even the conversations around it may be fabricated. The deeper concern in all this is not any single piece of synthetic media, but that as these technologies become easier to use and harder to detect, they slowly undermine individuals' ability to detect what is true and what is not. Consequently, this weakens the institutions citizens may rely on to verify or even obtain information, eroding trust in them (Ferrara 2026, 1).

The danger of fully artificial environments is accelerated by the “democratisation of disinformation”, as generative AI tools have completely distorted the information environment (Feuerriegel et al. 2023, 4). Once restricted to well-resourced organisations or state actors, the creation of large-scale false information has become accessible to anyone with minimal financial barriers. This democratisation amplifies the volume of disinformation while reducing its cost, complicating traditional detection strategies that are typically reliant, among other things, on platform moderation.

Moreover, as synthetic outputs become widespread, there is an additional risk that even authentic content may be dismissed as artificially created. This creates a ground in which uncertainty can be strategically exploited, enabling actors to deny allegations regardless of their validity. As a result, disputes become more difficult to resolve because even the basis of the evidence is questionable, leading audiences to scepticism. This results in what has been called the “epistemic tax”, where greater effort, time and resources are required to clarify or establish what happened, who said what and which sources can be ultimately trusted (Ferrara 2026, 7). This is associated with what is called the “liar’s dividend”, an issue that arises when malicious actors strategically weaponise the existence of AI to discredit authentic evidence by claiming it might be a deepfake or an artificially created image (Bontcheva et al. 2024, 13).

Finally, hyper-targeted persuasion and micro-segmentation, as discussed, enable the creation of personalised influence campaigns at scale. Therefore, instead of broadcasting a single, common narrative to millions, adversaries can create multiple narratives for small, targeted segments. These can be optimised to exploit different fears, identities, or grievances. Over time, these dynamics contribute to increasing division and, consequently, feed polarisation. Distinct groups are guided toward incompatible ways of interpreting reality, each influenced by seemingly credible synthetic evidence (Ferrara 2026, 6).

5. Case Studies

The following chapter provides an overview of election interference in Germany and France. By mapping the landscape and disinformation methods used to destabilise the democratic process of fair and free elections, the chapter aims to conclude overlaps in disinformation dissemination. Similarities and conclusions help to develop counter-measures to effectively combat future interference.

5.1 Germany’s Fertile Ground for Disinformation

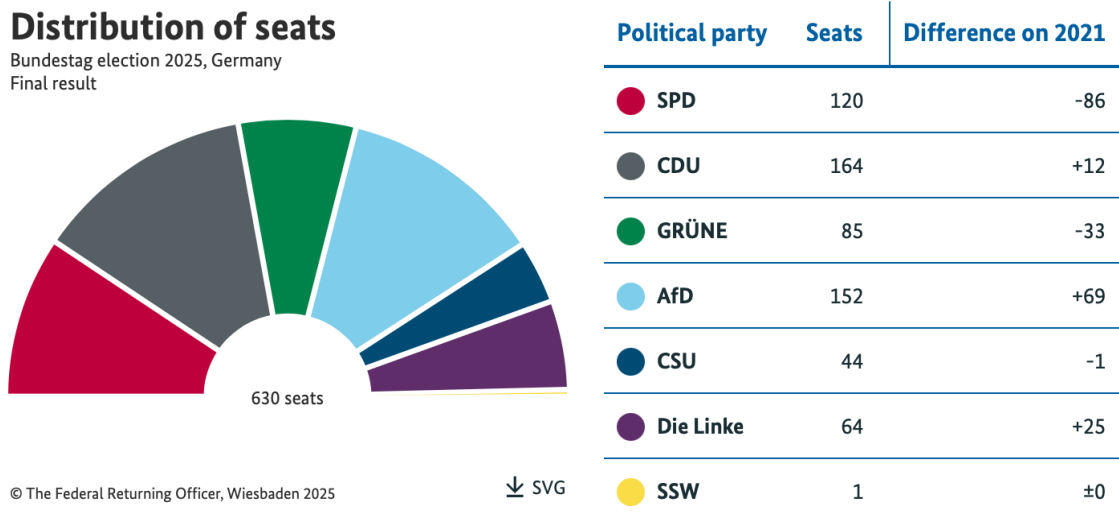
In the past five years, Germany has held two federal elections, both of which were marked by socio-political divisions and disinformation tactics used to deepen the social disconnect among voters. Elections were held in September of 2021 and February 2025, both resulting in very different outcomes. In 2021, the COVID-19 pandemic seemed to be largely under control, as infections had significantly decreased. Government restrictions had proven

effective, and the health crisis was not a main priority on the political agenda. Nonetheless, the management of COVID polarised public opinion. While some supported restrictions and vaccination campaigns, others opposed them heavily. Those against government intervention were part of a movement calling themselves “Querdenker”, “lateral thinkers” (Rensmann and de Zee 2022, 69-70). The movement was composed of “No Vax” activists, people sceptical of modern medicine, and right-wing extremists opposed to democratic systems (2022, 70). The new movement, combined with disinformation, further amplified societal divisions (2022, 75), while the far-right party Alternative for Germany (AfD) was gaining political momentum by campaigning on social media and presenting itself as a defender of the German people and their freedom (2022, 78). The election in 2021 resulted in the country’s first traffic light coalition, making three parties, the SPD (Social Democratic Party of Germany), Alliance90/The Greens and the FDP, the governing force.

Following the collapse of Germany's three-party coalition, new elections were set to be held in early 2025. The coalition's failure was met with great discontent among the public. The country was struggling economically, further deepening political and societal divisions within its society. In light of these circumstances, the 2025 Bundestag elections were deemed particularly susceptible to disinformation and election interference by foreign actors (Institute for Strategic Dialogue et al. 2023, 12-13). Alternative narratives that had already been present in 2021 further fragmented media landscapes and public opinion in Germany.

Election results show a big difference in voting between 2021 and 2025. The AfD, standing for alternative narratives, is a clear winner, gaining 69 seats in the Bundestag. The only other party that has more seats is the CDU.

Fig. 3: Distribution of Seats in the Bundestag, 2025 Compared to 2021



(The Federal Returning Officer Germany 2025).

At this moment, Germany is governed by a coalition between the CDU/CSU and SPD.

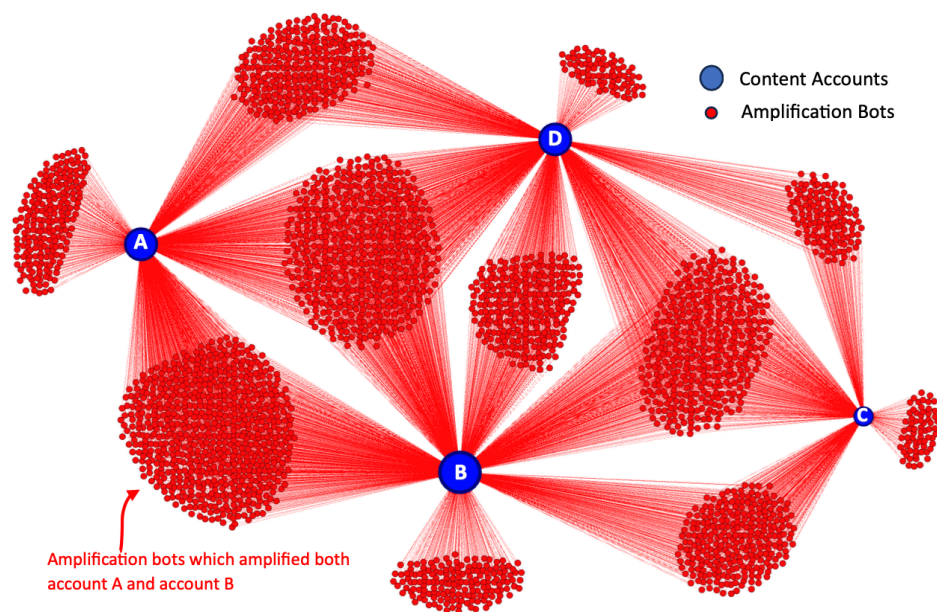
5.2 Targeted Smear Campaigning and Deep Fakes Dominate Electoral Periods

The German federal elections in 2021 and 2025 were both marked by disinformation campaigns, although the narratives and tools evolved. In 2021, disinformation methods were primarily characterised by efforts to undermine mainstream media and scientific expertise, particularly public health institutions. In the context of the election and the rise of the Querdenker movement, disinformation further reinforced existing scepticism. Disinformation narratives targeted public health experts, vaccinations and government restrictions, fuelling resentment against the government as a whole (Strategic Institute 2025, 42).

Leading up to the 2021 elections, one of the central streams of disinformation focused on electoral integrity and targeted individual candidates (2025, 31). DisInfo (2023) has identified five key disinformation narratives circulating prior to the election. Generally, the Greens and one of their party leaders, Annalena Baerböck, were targeted. Narratives included climate-related hoaxes, through messaging that emphasised the German way of life, would suffer under the green transition and personal disinformation attacks against candidates of the party. In addition to this, alternative health beliefs and “No Vax” ideologies gained traction. Furthermore, narratives around the war in Ukraine emerged and promoted the idea that

support for Ukraine should be heavily reduced. At the same time, disseminated disinformation amplified concerns over electoral integrity, alongside the spread of targeted smear campaigns as mentioned above (DisInfo 2023, 4-6). These attacks were carried out through highly coordinated disinformation campaigns (Federal Foreign Office of Germany, 2024, 22). This was executed by the distribution of posts on X (formerly Twitter) via automated systems, including amplification bots.

Fig. 4: Automated Content Distribution Systems



(Federal Foreign Office Germany 2024, 13).

In the figure above, the technical operation process of the automated content distribution system is shown. The blue dots represent individual content accounts, which are in reality synthetic identities. The red clustered dots are amplification bots that serve to increase engagement with the content accounts spreading disinformation. Such distribution systems allow for a rapid spread of published content, therefore reaching a wide audience. It is an ecosystem of disinformation channels that ensures the distribution of disinformation on social media platforms.

Such bots operate through interconnected accounts, enabling the simultaneous amplification of content at a high speed and scale (2024, 13). This disinformation strategy was used to both discredit certain parties and politicians and to endorse others through the same mechanism (Bundesamt für Verfassungsschutz n. d.).

By the 2025 election, both the intensity and the technological sophistication of disinformation had increased significantly. The Institute for Strategic Dialogue (2025) has identified AI as one of the key tools used by foreign actors to disseminate disinformation. One of the most prominent tactics was the use of deepfakes, particularly in video format (2025, 58). It should be noted that AI-generated audiovisual content had not been extensively studied in Germany prior to 2025. However, during the 2024/25 election period, multiple instances of AI-driven interference were recorded by the government and the Institute of Strategic Dialogue (2025, 35). For instance, fabricated videos circulated during the 2025 campaign, claiming that the AfD was missing as an option from ballot sheets, while other campaigns depicted ballots supporting AfD as destroyed. The campaigns were initially uploaded on X (formerly Twitter), by inauthentic accounts/bots and subsequently amplified by real users reposting the fakes (Institute for Strategic Dialogue 2026, 14).

During both election campaigns, websites of German news outlets were cloned, as reported by the Institute for Strategic Dialogue and the German Federal Office as part of the Doppelgänger campaign. Legitimate media outlets were imitated, including their design and typography, making them nearly indistinguishable from the authentic media outlet. Hundreds to thousands of articles were published disseminating false political content as well as false personal claims against candidates. One of the few noticeable differences was the domain name; while legitimate German outlets typically use .de, the cloned website would use alternatives such as '.ltd', or '.net'. In addition, the cloned sites included internal linking and redirected users from the cloned sites to the corresponding legitimate media platforms (Federal Foreign Office 2024, 6). Overall, disinformation in the German electoral context centred on the aforementioned themes, which included destabilising electoral integrity and aiming to weaken political actors, namely Annalena Baerböck from the Alliance90/Green Party.

5.3 From Trusting the Public to a Coordinated Task Force

During both elections, the German government was aware of disinformation and informed the public about common disinformation narratives. In 2021, the government issued informational materials to alert citizens to the spread of disinformation during the election

and to help them spot it. Attention was also called to possible influence from other states (Ministry of Interior and Community 2021, 2-5).

The FDP proceeded to submit a motion highlighting the possible risks of disinformation and cyber-attacks for the 2021 federal election. It warned that foreign actors, particularly from authoritarian non-EU states, may attempt to interfere to influence outcomes and destabilise the democratic process of the election. The party emphasised vulnerabilities in digital campaigning, including IT security risks for candidates and parties. Concerns over foreign donors were also raised. The motion finally called for stronger transparency in political advertising, aligned with the EU's Digital Services Act and a special task force to increase resilience against disinformation and other hybrid threats. Ultimately, the motion was denied (Deutscher Bundestag 2021).

The German government, therefore, did not establish a dedicated body to monitor and prevent disinformation. Instead, their approach focused on public information efforts. Responsibility during elections was largely assigned to the Federal Returning Officer. At the same time, social media platforms were said to be responsible for content on their applications, while the German State Media Authority should conduct further examinations and oversight (Bundeswahlleiter 2021).

In 2025, the government reported having built a task force to combat electoral interference for the federal election in 2025. The Ministry of Interior and Community acts as the central authority, collaborating closely with the Federal Foreign Office, the Federal Chancellery, the Federal Press Office and German security authorities to safeguard elections against external interference. Further, the Federal Office for Information Security supports political parties in security matters. The German government repeatedly emphasises the importance of transnational cooperation, and is partnering with the EU and other international partners to address disinformation and potential threats (Federal Government of Germany 2024). At this time, there is no official evaluation published by the German authorities measuring the effectiveness of the 2025 safeguarding measures. Specific disinformation campaigns are analysed by the Institute for Strategic Dialogue in cooperation with the German government and the EU, but no comprehensive report on effectiveness is available.

5.4 Disinformation Exploiting Crisis and Fear in France

France is the second most targeted state after Germany with respect to disinformation (EUvsDisinfo 2021). France has held two national elections in 2017 and 2022, both of which have been characterised as intentional attempts to target the French state and its electoral processes. The lead-up to the 2017 national election was a period of significant volatility as France grappled with terrorism and polarisation, economic stagnation, and a breakaway from the traditional left-right political establishment.

Several terrorist attacks in France from 2015-2016, including the Charlie Hebdo shooting, the November 2015 Paris attacks, and the July 2016 Nice truck attack, claimed the lives of more than 230 people (Chatignoux et al 2018, 413). In response to these attacks, the French government, led by then-President François Hollande, implemented and extended a state of emergency which banned public demonstrations, permitted police to conduct searches without a warrant, and blocked websites that encouraged acts of terrorism (Lawfare 2015). During this period, issues of security, terrorism, and the role of Islam in French society were top political campaign issues. Between 2015 and 2016, the increased movement of refugees and migrants seeking asylum in Europe, coupled with multiple terrorist attacks in France, created a climate of high social polarisation in which the far-right Front National, led by Marine Le Pen, was able to consolidate support.

Furthermore, economic stagnation and high unemployment, particularly among youth in the lead-up to the 2017 national election, created a sense of public dissatisfaction and the sentiment that the then French political establishment of centre-left (Parti Socialiste) and centre-right (Les Républicains) was out of touch with the French electorate's lived realities. For the first time in the history of France's Fifth Republic, established in 1958, the top two presidential candidates represented political parties outside the mainstream - Emmanuel Macron representing the new En Marche! movement and Marine Le Pen of the Front National (Congressional Research Service 2017, 1).

Political polarisation, a fragmented party system, and social divisions based on French identity, education, and economic status defined the period leading up to the 2022 national election. Concerns around immigration and national security remained pervasive, which Marine Le Pen's far-right National Rally party capitalised on to challenge President Macron's

more centrist movement. This time period also introduced a new sense of polycrisis between the COVID-19 pandemic and the war in Ukraine. Economically, French voters were concerned with inflation and the rising cost of living, along with proposed reforms to retirement age. Social discontent remained high, especially during the Gilets Jaunes (Yellow Vests) protests from 2018 to 2020. The Gilets Jaunes movement began as an anti-tax protest against the rising price of petrol and was amplified when some protests, especially in Paris, led to violent confrontations between the Gilets Jaunes and the police, during which the police were accused of using unnecessary force (Freedom House 2019). It is important to note that what underlies the Gilet Jaunes' protests is the frustration that President Macron's administration was out of touch with the realities of French daily living. For example, outside of the major metropolitan areas of Paris, Bordeaux, or Marseille, rural or outer-urban areas experienced a decline in public service provisions and commercial services, such as a lack of access to doctors or closures of post offices (Hewlett and Kuhn 2022, 395). These dynamics, coupled with existing wealth inequality, paved the way for demographic divides in which voting patterns reflected that younger, less educated, and blue-collar workers were more likely to support the far-right National Rally. While President Macron attempted to respond with concessions, social dissatisfaction remained high. Later in this report, we will see how foreign actors sought to exploit existing social tensions in France through targeted disinformation.

5.5 From Data Hacking to Long-Term Manipulation Operations

Disinformation in French elections has been characterised by targeting candidate reputations, electoral integrity, and data hacking and leaks. In contemporary French politics, the 2017 presidential election demonstrated the largest failed attempt by foreign actors to interfere in electoral processes known as the “Macron Leaks”. In May 2017, two days before the second and final round of the French presidential election, approximately 21,000 emails from Emmanuel Macron's presidential campaign team were hacked, including emails from Macron himself, and subsequently leaked onto a 4Chan forum (Vilmer 2018, 76). Once released, the “Macron Leaks”, which included a combination of real emails and forgeries, were then quickly posted by pro-Trump and pro-Russian social media accounts and by WikiLeaks. Intended to prompt a last-minute scandal against Macron's presidential campaign, the hack-and-leak operation took place right before the French electoral silence, a legally mandated 48-hour period of silence between media and political campaigns intended to

prompt reflection (Vilmer 2018, 77). The Macron campaign swiftly intervened before the start of the electoral silence, issuing a press release that “the movement has been the victim of a massive and coordinated hacking operation” (En March 2017). It is important to note that a series of disinformation operations were employed well before the 2017 election against Macron’s campaign team, as well as against other French electoral infrastructure.

Earlier in 2015, a cyber-attack against the French television network, TV5Mondewas documented, including reconnaissance of the network’s systems and the installation of malicious software, which then cut the network’s broadcast television programs (Kondratev and Johansson-Nogués 2022, 13). Warnings of further attacks were posted to TV5Monde’s Facebook account, and inflammatory messages alluding to existing social tensions in the wake of the Charlie Hebdo terrorist attacks were clear. Soon after, new hybrid interference campaigns targeting the French state and its electoral processes took place to which the French Defence Minister, Jean Yves Le Drian, warned, “by targeting the electoral process of a country, we are undermining its democratic foundations, and therefore its sovereignty” (Le Journal du Dimanche 2017).

In early 2017, once it became clear that Emmanuel Macron would be a leading candidate for the presidential election, disinformation attacks against Macron and his political campaign team intensified in comparison to criticisms against fellow candidates, Francois Fillon and Marine Le Pen (DFRLab 2017). Foreign publications with ill intent published stories that the founder of WikiLeaks, Julian Assange, would release memos stolen from the US Democratic National Committee in 2016 that were damaging to Macron (Kondratev and Johansson-Nogués 2022, 13). Furthermore, these same maligned publications published attacks of both political and personal nature, ranging from narratives of Emmanuel Macron as an American spy, alleged “homosexual orientation”, and having received funding support from Saudi Arabia and the Rothschild family (EUvsDisinfo 2019). As the influx of disinformation continued, Socialist MP Richard Ferrand commented out of concern on trust in French electoral processes, “False information from [foreign media] is weighing on [France’s] democratic life” (Vinocur 2017).

In 2018, at the height of the Gilet Jaunes protests, several studies suggested that foreign actors were responsible for spreading and amplifying disinformation to the movement through traditional and social media channels. Evidence ranged from one maligned foreign

publication accumulating more video viewership related to the Gilet Jaunes protests than five French publications combined, with one-sided coverage (Kondratev and Johansson-Nogués 2022, 14). Related to disinformation during these protests, these maligned publications also falsely claimed that the majority of French police no longer supported Macron and circulated manufactured videos of police in solidarity with protesters. The police authorities involved denied this activity, and one of the maligned publications was then forced to issue a correction. Given how this particular disinformation campaign sowed doubt about political leadership and easily exerted influence on the democratic system, the French government intervened by investigating the maligned publications' links to foreign governments (Matlack and Williams 2018).

The 2022 presidential election exhibited more sophisticated means of disinformation, ranging from an uptick in fake narratives, misleading content, and perhaps most importantly, manipulated video content through deepfakes. Where the 2017 presidential election centred around a singular “hack and leak” operation via the Macron Leaks, the 2022 election showcased that foreign actors were now focused on longer-term manipulation operations. Several false claims were spread during the 2022 election campaign, which were intended to sow distrust in French electoral processes. These include the hoax that over 22,500 Gilets Jaunes would have been barred from voting due to a 2020 law (AFP France 2022). Mimicking “Stop the Steal” rhetoric in the US, rumours were spread that an American company, Dominion, played a role in rigging French voting machines, which was false (AFP France 2022). During the election broadcast on French news channel France 2, the network’s software for live graphics malfunctioned, which inflated the number of votes for Marine Le Pen and screenshots from that live TV malfunction were then circulated online to falsely suggest that two million votes for Le Pen “disappeared” during the election count (EU Disinfo Lab 2022). By June 2023, the French General Secretariat for National Defence and Security (SGDSN) confirmed “Doppelgänger” campaigns clearly linked Russian operations to a major disinformation campaign. The SGDSN reported that leading French media websites like Le Monde, Le Parisien, Le Figaro, and 20 Minutes were imitated to then spread fake news about the war in Ukraine (SGDSN 2023). The “Doppelgänger” campaigns revealed overt anti-Western and anti-Ukrainian sentiment.

Targeting electoral integrity, smear campaigns, and the hack-and-leak operations of the 2017 election, along with the advent of fake narratives and deepfakes in the 2022 presidential

election, illustrate the progression of disinformation aimed at destabilising the democratic process in French elections. Similarly coordinated efforts were reported during the 2024 European Parliament election, as “Doppelgänger” campaigns once again mimicked French media outlets such as “Le Monde” and “Le Figaro”, aiming to spread anti-Macron narratives in favour of National Rally figures like Marine Le Pen and Jordan Bardella. Foreign actor bots also launched a disinformation campaign on X (formerly Twitter), intending to overwhelm the social media platform with “Doppelgänger” articles to amplify the French far right. During the June 2024 French legislative elections, deepfake videos were pervasive, depicting relatives of political figures like Marine Le Pen and were widely shared on social media platforms to heighten France’s existing political polarisation (EU Disinfo Lab 2025). France is actively preparing for disinformation campaigns targeting the upcoming presidential elections, with a particular focus on strengthening its defence capabilities and surveillance mechanisms.

5.6 A “Diplomacy of Combat” Approach

In response to growing threats of disinformation, France has taken a “diplomacy of combat” approach by actively monitoring and exposing malicious narratives as well as implementing regulatory actions and social media counter-influence (France 24 News 2022). Institutionally, the French government established Viginum in July 2021, a dedicated division within the General Secretariat for National Defence and Security (SGDSN) to deter and counter foreign digital interference intended to undermine democratic stability. Viginum monitors digital platforms for manipulative content, with a particular focus on coordinated, foreign-backed campaigns that target electoral integrity rather than domestic interference. With an eye to safeguarding privacy rights and freedom of speech, Viginum’s work is supervised by the inter-ministerial Ethics and Scientific Committee within the SGDSN and is strictly regulated by French law. In the 2022 elections, Viginum was credited with identifying five verified foreign interference campaigns (Diossy et al. 2024, 7).

In terms of legislative measures, the French government passed the “Law on the Manipulation of Information” in December 2018, which allows candidates and political parties to appeal to a judge to stop the spread of false information during the three months leading up to a national election. As an “anti-fake news” law, it allows judges to take urgent measures against internet service providers to stop the spread of false information. The 2018

law requires digital platforms with over five million users to combat fake news by providing tools for reporting false information, improving algorithmic transparency, and combating malicious accounts. France's recently merged audiovisual regulator, the Authority for the Regulation of Audiovisual and Numeric Communication (ARCOM), enforces legal obligations on social media platforms, like the 2018 Information Manipulation Law, to help curb the spread of fake news. Launched in 2022, ARCOM has the authority to suspend foreign-controlled media outlets if they intentionally propagate false information that could affect election integrity (EU DisinfoLab 2022). Lastly, France is a signatory to the European Union's Digital Services Act (DSA) and ensures compliance by social media platforms, especially regarding electoral disinformation.

In line with its “diplomacy of combat” strategy, the French government has more recently taken a cultural approach to fight back against disinformation. In 2025, the French Ministry for Europe and Foreign Affairs launched “French Response”, an official account on X which aims to use humour, irony, and a mix of memes, images, facts, and figures to undermine disinformation and proactively call out foreign interference campaigns (France in the United Kingdom 2026). By leveraging humour and irony, the “French Response” is not only able to verify facts, but the initiative is also able to make manipulative information present as ridiculous, thus reducing public susceptibility to believing hostile propaganda and the likelihood of such information going viral. The “French Response” signals a shift in France's online strategy to be more proactive in shaping its own narratives amidst what can otherwise be an antagonistic information space.

5.7 Cross-Case Findings: Germany and France

Germany and France present several similarities in elections ranging from 2017 to 2025. Firstly, the sociopolitical environment of polarisation heightened the frustrations of communities deemed on the “periphery” in German and French societies. During the COVID-19 pandemic in Germany, the cross-border “Querdenker” movement strongly opposed government-led public health interventions and the status quo of democratic systems. With false narratives on the rise, fueling “Querdenker” scepticism against vaccinations and public health expertise, disinformation campaigns amplified societal divisions separating those who maintained trust in government against those who sought alternatives. In this context, the far-right AfD gained political momentum by claiming to

“defend the German people and their freedom”. In neighbouring France, the “Gilet Jaunes” movement arose from protests against the rising cost of living, namely inflation, and from frustration that the Macron administration was out of touch with the lived realities of rural and outer-urban communities. Disinformation exacerbated polarisation, sometimes leading to violence between protesters, police, and journalists reporting on these incidents. It is said that those who supported the “Gilet Jaunes” movement were more likely to support the far-right National Rally. While the platforms of the “Querdenker” and “Gilet Jaunes” movements were very different in their advocacy, the spread of disinformation reinforced social tensions and may have laid the groundwork for far-right political campaigns to gain influence.

New political developments also emerged, which challenged the existing political infrastructure in Germany and France. For the 2021 German election, which resulted in the country’s first light coalition, making three parties, the SPD, the Greens, and the FDP the governing force, the 2017 French election also experienced its first break from the traditional political establishment when the top two presidential candidates, Macron of the En Marche! Movement and Marine Le Pen of the Front National, both represented political parties outside the mainstream. Furthermore, in the 2025 German election, the AfD gained 69 seats in the Bundestag, a first for the right-wing party. The 2024 French legislative election illustrated similar dynamics, with the right-wing National Rally having gained 52 seats, an unprecedented feat for the party in terms of MP numbers (BBC News 2024). As a result of this shifting political landscape of a fragmented, multi-block structure, both the contemporary contexts of Germany and France reveal the challenges of majority-based governance and require openness to new alliances to maintain power.

Related to disinformation methods in elections, the German and French elections share similar narratives with respect to anti-government stances, the spread of anti-refugee/immigrant sentiment, as well as the implementation of smear campaigns against candidates and Doppelgänger campaigns. Disinformation in both the German and French contexts has amplified concerns over electoral integrity as smear campaigns have intended to discredit some political candidates while endorsing others. In the 2017 French election, Macron was the clear target for disinformation tactics while false narratives were presented favourably for Marine Le Pen and the National Rally. In the 2021 German election, gendered disinformation played a prominent role in the pushback against Green Party candidate for Chancellor and German Foreign Minister, Annalena Baerbock. The attacks against Baerbock

ranged from both political and personal nature, similar to Macron's experience in the 2017 election. Given Baerbock's identity as a woman, several studies have found that Baerbock was disproportionately targeted in comparison to her male competitors with disinformation campaigns, including sexist and gender-based narratives, in addition to false accusations regarding her policies. These campaigns have been attributed to foreign interference (EU DisinfoLab 2023, 5). Lastly, both Germany and France saw the progression of AI as a tool for disseminating disinformation, especially the rise of deepfake videos with false claims uploaded by bots and then amplified by real users reposting false information on social media platforms. "Doppelgänger" campaigns mimicking legitimate media outlets are prominent in both German and French elections, including the false claim that ballots supporting the AfD were destroyed in Germany and that two million votes for Le Pen and the National Rally disappeared in the election count during a live TV malfunction in France.

The primary differences identified between France and Germany were diverging from each other by way of operation. While Germany, during the 2022 federal election, emphasised informational material and did not form a government section to oversee disinformation and electoral interference, France spread responsibility among its institutional bodies. France passed a law on information manipulation in 2018, allowing parties to appear before judges to appeal the circulation of disinformation in the three months prior to the election. This safeguarded fair elections through judicial avenues in subsequent years.

In 2025, France and Germany followed a more similar path in combatting disinformation in efforts to effectively safeguard its democratic processes. While the latter introduced its own task force focused on interference, specifically targeting the federal election of 2025, France launched Viginum within SGDSN and ARCOM, which serve as regulatory and oversight bodies. The two bodies are not situated within the same institutional sector, which allows for broader oversight.

6. Swiss Landscape Analysis

The following chapter provides insight into the Swiss information environment, detailing the contemporary risk landscape of information manipulation and disinformation in Switzerland, listing and critically discussing existing disinformation countermeasures, reviewing comparative lessons from Germany and France, and providing concise recommendations customised for Switzerland.

6.1 Switzerland's Media Environment: Stable but not Exempt

Switzerland, as a case, stands as a paradox. It ranks among the most institutionally trusted democracies while also experiencing a measurable, accelerating deterioration of its information environment (OECD 2024). While neither of those claims alone captures the complexities of Switzerland, it is precisely the acknowledgement of the coexistence of structural resilience and specific vulnerabilities that is highly relevant to identifying functional, realistic resilience mechanisms and strategies applicable to Switzerland.

According to the OECD (2024), 62% of Swiss adults reported high or moderately high trust in the federal government in 2023, which lies nearly 23% above the 30 surveyed countries' average of 39%, high or moderately high levels of trust are also present in different institutional categories such as, trust in police (75%), judicial system and apparatus (69%), civil servants (56%), and local government (63%), while political parties (38%) and news media (40%) demonstrate the least highly and moderately high trust levels in governmental institutions in Switzerland. More than half of the Swiss adult population (58%), thinks that their will and political agenda finds representation and is actionable in the Swiss political system. According to the OECD (2024), this stands both as a strong indicator and driver of trust in government, considering that the average score in high to moderate trust levels in surveyed countries is 30%. This cross-border analysis of information environments situated Switzerland within the “media-supportive, consensual” cluster of European democracies, characterised by the highest degree of systemic resilience to disinformation (Humprecht et al. 2020, 16). Additionally, the Swiss Federal Council considers Switzerland less prone to disinformation operations due to a high standard of living, high levels of education, strong popular confidence in state and media institutions, political competence fostered by frequent

referendums, linguistic and cultural diversity, and “low geopolitical relevance” (Federal Council 2024, 14).

Nonetheless, Switzerland is experiencing a downward trend, as evidenced by surveys by the Swiss Statistical Office, which found an increase in the prevalence of disinformation in users' social media feeds from 45% in 2021 to 51% in 2025 (BFS 2025). Declining trust in Swiss media and institutions (from 50% in 2016 to 42% in 2023) aligns with statistics across EU member states, confirming a cross-border downward trend (Federal Council 2024, 16).

Switzerland might not be at the same risk level as other democracies due to its high baseline of institutional trust, thus making it more resilient to potential pressures but not immune. This notion is also represented in both France and Germany, as both demonstrate that high baseline levels of trust in media and governmental institutions alone do not fully shelter democracies against the impact of lasting foreign or domestic influence operations, signifying the importance of both high trust in institutions and institutional architecture that can monitor, attribute and respond to threats at the operational quality and tempo at which they evolve and spread (Federal Council 2024, 4-6; North et al. 2024, 4).

6.2 When Democracy becomes a Vulnerability

Systematic, geopolitical, and domestic-political factors shape Switzerland's threat landscape, which is qualitatively distinct from both Germany's and France's. The following will detail these three threat vectors before moving to existing Swiss countermeasures and to comparative lessons that Switzerland can draw from the aforementioned cases and prior experiences in the domain of disinformation and democratic resilience.

One of the core pillars of Swiss democracy is its direct democratic system, which produces a comparatively high frequency of elections, creating recurrent, predictable windows of vulnerability for the Swiss state and opportunities for influence campaign actors. This vulnerability is acknowledged by the Swiss Federal Council and described as giving actors the ability to “exert influence on a case-by-case basis” (Federal Council 2024, 14-15). Switzerland's political landscape, issue-attitude congruence, and heavy social media use are identified as the primary individual-level drivers of disinformation dissemination, suggesting

that the problem is motivationally and institutionally based rather than primarily epistemic (Morosoli et al. 2025, 3-4).

Morosoli et al. (2025) findings are confirmed through case-specific data on the dissemination of disinformation during the first COVID-19 wave in 2020. Baumann and Humprecht (2025), illustrate that disinformation was more frequently shared than accurate information on ‘Swiss Facebook’, with right-wing actors and alternative media accounts functioning as the most prolific disseminators. The Swiss Federation has established processes to counter the spread of disinformation in referendums or election settings, such as media monitoring, election-related risk assessments at the federal and cantonal levels, and counter-campaigns, but falls short of establishing counter-strategies that depart from traditional “informative/fact-checking/intervention” approaches and aim for sustainable change in options on the part of disinformation disseminators, as rebunking an already established belief proves less efficient than pre-bunking (Van Der Linden et al. 2026, 2).

6.3 Interference from Abroad: Switzerland as a Geopolitical Target

Switzerland, as a host of United Nations Organisations, financial institutions and NGOs, means that successful operations can have consequences that reach far beyond Swiss domestic politics, thereby making Switzerland vulnerable to foreign disinformation actors. State actors are the primary international threat actor within Switzerland's hybrid threat environment, a conclusion corroborated by multiple sources (Federal Intelligence Service FIS 2024; Federal Council 2024; Federal Intelligence Service FIS 2023; Federal Council 2021; European Commission 2023, 2025; Vogler et al. 2021). The Swiss Federal Intelligence Service (2024, 64) states that the greatest hybrid threat to Switzerland stems from foreign state actors. This hybrid threat is not limited to espionage per se. Hybrid threats encompass propaganda and covert influence operations, which entail disinformation. The aforementioned report notes that “the escalating power political confrontation worldwide has increased the hybrid threat to countries, including Switzerland, in particular from external influence activities” (Federal Intelligence Service FIS 2024, 13). External targeting of Switzerland is partly due to its alignment with European Union sanctions against certain states, which led to its classification as an “unfriendly state”. Simultaneously increasing the scale and intensity of targeted disinformation operations, such as during the 2024

Geneva-based peace talks, with the goal of both undermining Swiss public opinion and destabilising the credibility of Swiss institutions (Federal Council 2024, 5-13).

The European External Action Service's (EEAS) annual report on Foreign Information Manipulation and Interference (FIMI) corroborates Swiss-based findings documenting that external FIMI operations represent a sustained effort in “build[ing] a False Façade to hide pro-Kremlin information laundering operations or to impersonate legitimate media outlets in order to co-opt their credibility” (European Commission 2025, 12). For example, the operation “Doppelgänger” targeted European Union audiences, but also reached Swiss audiences because of linguistic and information consumption proximity and the cross-border characteristic of the internet and digital media (Federal Council 2024, 6). This further illustrates the cross-border nature, specifically in digital disinformation operations.

The fourth EEAS FIMI Report (European Commission 2026) provides insight into the scale of contemporary operations directed at Europe and elaborates that in 2025, FIMI targeted elections in Germany, Poland, Romania, Czechia, Moldova and Côte d'Ivoire, while 29% of all documented FIMI incidents were attributed to Russia. This illustrates continued operational intent and a system of interference targeting European democracies and their elections in general. Switzerland's periodic election cycle and central geopolitical position make it a major target of influence operations, yet it lacks the infrastructure response architecture and ability present in NATO or the EU's collective “Rapid Alert Systems” (Federal Council 2024, 10).

Furthermore, Switzerland lacks any central coordination or counter-measures agency, acknowledging that “almost all administrative units can be affected” by information operations, while calling for the establishment of a responsible governmental actor to simplify counter-measures and legislation aimed at increasing democratic resilience (Federal Council 2024, 23). This, combined with continued technological innovations in AI- and related technologies, enables increased scale and speed of operations while costs remain minimal. This poses yet another risk factor within the geopolitical threat vector, as it enables intensified operations without increasing burdens on the propagator, allowing non-state actors to operationalise strategies formerly vested in state actors who had the capacity to back such operations (European Commission 2025, 11).

6.4 Domestic Threat Vectors

While foreign states are the primary threat to Switzerland's information environment, domestic actors facilitate disinformation or disinformation-aligned communication within the Swiss public sphere. Through legitimate political channels or fringe German- and French-language cross-border media outlets, they often carry the institutional and cultural credibility that foreign campaigns cannot easily emulate.

Party political actors, a transnational German-speaking alternative media ecosystem and the structural opportunity created by Switzerland's high-frequency referendum calendar are the key interconnected threat vectors present in the Swiss domestic context. The year 2023 marked the normalisation of AI-assisted manipulation into the mainstream of Swiss political campaigning. In July of the same year, the FDP *Die Liberalen* (FDP) published an AI-manipulated poster depicting a fabricated scene of climate activists obstructing an ambulance. Similarly, the Swiss People's Party (SVP) parliamentarian Andreas Glarner published a deepfake video portraying the Green MP of Turkish origin, Sibel Arslan, saying "I want all criminal Turks to be deported!" (Bernhard 2024, 4).

These two cases made it clear that synthetic manipulation targeting political opponents was no longer a fringe practice on the political periphery, but rather a tactic used by elected federal parliamentarians for political gain. Other political parties represented in the Swiss parliament, later that same year, signed a voluntary code of conduct limiting the use of generative AI in their political communication. FDP and SVP did not sign the agreement (Strasser 2023).

Alternative media environments and publishers can be described as journalism-seeming publishers that do not adhere to journalistic codes or are bound by legislation aimed at journalistic organisations. Publishers can amplify and produce domestic disinformation while having financial incentives to increase viewer numbers, without the institutional checks and balances present in traditional media environments (Faris et al. 2016, 36; Marwick and Lewis 2017, 45). Alternative media outlets and social media influencers are identified as the primary disseminators of disinformation, while increased rates of consumption are also an indicator for "reduced resilience and increased willingness to circulate disinformation" (Humprecht et al. 2023, 5).

Conversely, this means that the critical consumption of legacy media can increase resilience to disinformation. It is also important to note that alternative media ecosystems do not stop at borders; communities of alternative media consumers can be found in cross-border contexts in which narratives and sentiments travel along linguistic rather than border lines. In other words, the shared consumption of German alternative media can have different effects across national contexts. Finally, Switzerland's direct democracy, characterised by frequent elections and referendums, makes the persuasion of the majority secondary, as even a marginal doubt can lead to considerable changes in attitude (Federal Intelligence Service, 2024).

6.5 A Fragmented Shield: Switzerland's Counter-Disinformation Architecture

Switzerland's current anti-disinformation strategies are rooted in existing policies, drawing on constitutional, criminal, and sector-related legislation and provisions (Thouvenin et al. 2024, 8). Free and unmanipulated expression and formation of political will and opinion are guaranteed under Article 34/2 of the Federal Constitution, while Article 36 outlines restrictions on the expression of opinions, such as slander, defamatory or discriminatory statements (Federal Council 2024, 17).

Criminal law provides legislation on the intimidation of the population (§258 Criminal Code), discrimination or incitement to hatred (§261 Criminal Code), attacks on the constitutional order (§275 Criminal Code) and offences against the popular will can be invoked where discrimination crosses into unlawful conduct (§279 Criminal Code) (Federal Council 2024, 17-18). Foreign donations to political movements and groupings are prohibited under Article 76h of the Federal Law on Political Rights, making externally funded causes illegal (Federal Council 2024, 15).

At this moment, no institutionally grounded central coordination body exists in Switzerland; responsibility is spread over multiple agencies, with the Security Core Group reviewing influence activities at least twice per year, and an inter-departmental network of contact persons, while the Department of Foreign Affairs conducts cross-department workshops educating relevant personnel on the topic of influence activities and disinformation (Federal Council 2024, 23). In the run-up to the Federal elections in 2019 and 2023, the Federal Chancellery convened party representatives, digital media contact persons, the National

Cyber Security Centre and the Federal Data Protection Commissioner to arrange privileged channels with Google, Meta and ByteDance (TikTok) to flag manipulated content and increase coordination between state and private actors (Federal Council 2024, 23). While Switzerland and the European Union disagree on the question of sanctioning foreign state-sponsored publishers, the Federal Council commissioned the Federal Office of Communication (OFCOM) to discuss the consultation draft on a communication-platform regulation modelled on the EU Digital Services Act, to increase accountability of large digital information platforms such as Google, Meta, X or YouTube (Federal Council 2024, 21; Federal Department of the Environment, Transport, Energy and Communications 2025).

Civil society responses to disinformation remain comparatively limited but are still active. Self-regulating bodies such as: the Press Council, which enforces the code of journalists with the directive to seek truth (Wahrheitssuche), obliges journalists to verify and correct information. The Swiss Commission of Fair Trading adjudicates misleading commercials, and the Swiss Code of Conduct of Hosters regulates how intermediaries hosting misleading content online are ought to handle such content, all acting as soft-law mechanisms self-regulating specific industries and self-set standards (Thouvenin et al. 2024).

The popular *Internet Initiative* (Initiative) represents a recent civic effort to embed digital rights and platform accountability into the constitutional order, intending to increase accountability and limit the risk of manipulation and algorithmic amplification of democratic standards in the information age. Additionally, research institutions such as the Research Centre for the Public Sphere and Society (fög) inform the public debate and government officials annually about the quality of the media environment in the *Yearbook Quality of Media* (fög 2025).

Educational efforts that aim to counter the reach or impact of disinformation are distributed across federal, cantonal, and non-state civil society actors, all of which aim to increase media competencies, especially in the digital sphere (Thouvenin et al. 2024, 20). Educational efforts aimed at younger audiences have already been in place since 2022 in the form of Lehrplan 21, integrating modules on media literacy and computer sciences from kindergarten through lower secondary school on a federal level. Meanwhile, older audiences are not reached by state actors and are more likely to be reached by civil society actors who cooperate with state

actors in organising workshops and educational material online. On a federal level, the online portal “ch.ch” presents practical guidance aimed at limiting the impact of disinformation and drafting educational material on influence activities while also supporting and funding the *Open Education & Digital Competencies* programmes designed to support the education of both teachers and students with the aim of developing a digital culture in classrooms with a focus on digital media and AI (Federal Council 2024, 21).

7. What Switzerland is Missing: Institutional and Civil-Society Recommendations

Germany and France, although divergent in their threat profiles, institutional setups, and responses, converge on a diagnosis directly applicable to Switzerland: specifically, that a high-trust baseline and a strong media ecosystem do not, on their own, shield democracies from coordinated disinformation. Both initially relied on distributed responsibilities and general-purpose legal provisions, similar to current Swiss countermeasures, and concluded that this architecture was insufficient to match the operational tempo and scale of contemporary disinformation campaigns (Federal Government Germany 2024; SGDSN 2023).

France’s response to the growing risk of disinformation, namely the establishment of Viginum in 2021 as a dedicated unit within the National Defence and Security Secretariat, created a central accountable body mandated to detect, analyse and attribute foreign interference. This opposes Switzerland’s distributed resilience structure, made up of multiple actors and governmental institutions, responsible for detection, analysis, and attribution (Federal Council 2024, 23-24). Additionally, France enacted the Law on the Manipulation of Information in 2018, granting judges urgent injunctive powers during the three months preceding national elections and obliging social media platforms with more than five million users to maintain reporting tools, algorithmic accountability, and anti-manipulation mechanisms. The 2022 consolidation of ARCOM further strengthened the regulatory authority over audiovisual and digital communications, giving the body the power to control and, when deemed necessary, suspend foreign-controlled media outlets judged to threaten major national interests, and to call out actions, enabling the state to implement appropriate countermeasures that go beyond lip service. The launch of the *French Response* signals a purposeful shift from reactive debunking toward a preemptive narrative production, in line

with the pre-bunking logic identified by Van Der Linden et al. (2026) as more effective than corrective interventions after the fact.

Germany's case demonstrates a 2021 departure point similar to Switzerland's current posture. Its 2021 approach relied on public information campaigns and on dispersing responsibility among the federal Returning officer, the state media authority, and individual social media platforms. The 2025 pivot to vest central coordination authority into the Ministry of Interior and Community, convening the Federal Foreign Office, the Federal Chancellery, the Federal Press Office and the security services, while the Federal Office for Information Security extended direct IT support to parties and local governmental institutions, allowed it to respond directly to the 'hack-and-leak' vector that also materialised in France's 2017 Macron Leaks operation.

Taken together, four shared practices emerge from the two cases that are currently absent or underdeveloped in Switzerland. First, a designated agency with an explicit anti-disinformation and foreign interference mandate. Second, pre-election IT security support provided by institutions to political parties and candidates. Third, legally grounded platform obligations covering algorithmic disclosure, fast-track injunctive mechanisms and reporting duties. Lastly, institutionalised pre-election coordination between government, parties, platforms and regulators to minimise the risk of misinformation in a given context. The 2019 and 2023 meetings with platform officials from Meta, Google, and ByteDance constitute a prototype of the last practices, which could be formalised into a standing protocol rather than an ad hoc convening. The following table will summarise these outcomes:

Recommendations for Switzerland

Practice	France	Germany	Switzerland
Dedicated anti-disinformation agency	Viginum EU Rapid Alert System	Interior Ministry task force EU Rapid Alert System	<u>Not yet developed</u>
Pre-election IT support to parties	Arcom oversight	Federal Office for Information Security	<u>Not yet developed</u>
Platform legal obligations	Law on the Manipulation of Information DSA	DSA	OFCOM draft in preparation
Institutionalised coordination	SGDSN-led	Inter-ministerial task force	Ad hoc (Federal Chancellery)
Proactive narrative production and prebunking	French Response	<u>Not yet developed</u>	<u>Not yet developed</u>

8. Conclusion

Finally, this report identified strategies by which the Swiss Confederation, its democratic institutions, and civil society actors can strengthen their resilience against digital disinformation campaigns and related manipulative practices from both internal and external actors. The close analysis has revealed that Swiss vulnerabilities are neither primarily epistemic nor simply a consequence of insufficient citizen trust in institutions, but rather arise from the interaction between a high-frequency direct democratic calendar, an operationally fragmented counter-disinformation architecture and a technologically accelerating threat environment in which foreign state actors and domestic political actors increasingly converge on shared communication strategies and methods.

Germany and France illustrate that high institutional trust and strong legacy media are necessary but alone insufficient conditions for successful democratic resilience in the contemporary era, as both states initially relied on departmentalised responsibilities and general-purpose legal provisions, resembling Switzerland's current countermeasures, and both states concluded that this architecture could not match the operational tempo or scale of contemporary disinformation operations. France's 2018 Law on the Manipulation of Information, the establishment of Viginum in 2021, the 2022 consolidation of ARCOM, and the 2025 launch of the "French Response" social media accounts demonstrate a strategic move from reactionary debunking to anticipatory narrative production and legally grounded platform accountability. Similarly, Germany's pivot from 2021 to 2025, namely from a dispersed approach to responsibility to the Interior Ministry-led task force coordinating the Federal Foreign Office, the security services, the Federal Chancellery, and the Federal Office for Information Security, traces a similar trajectory from ad hoc responses on a case-by-case basis to an institutionalised resilience mechanism.

Four practices are currently absent or underdeveloped in Switzerland and constitute the core recommendations advanced here. Firstly, a designated agency with an explicit mandate to combat disinformation and counter foreign information manipulation and interference should replace the current status quo of responsibilities distributed across governmental institutions and federal bodies. Secondly, pre-election IT security support should be formalised for political parties and candidates and modelled on the services offered by Germany's Federal Office for Information Security. Thirdly, the OFCOM consultation draft on communication platform regulation, modelled on the European Union's Digital Services Act, should be advanced into binding law, establishing algorithmic disclosure requirements, fast-track injunctive mechanisms, and reporting duties. Lastly, the Federal Chamber's 2019 and 2023 convening of META, Google and ByteDance should be formalised into a standing pre-election coordination protocol rather than remaining ad hoc.

In addition to institutionally grounded changes, Switzerland should invest in civil society-led prebunking initiatives, building on evidence that pre-exposure to manipulation tactics is more effective than post hoc corrections (Van Der Linden et al. 2026). Existing educational efforts, such as Lehrplan21, the 'ch.ch' portal and the Open Education & Digital Competencies Programme, are reaching younger audiences while leaving older cohorts comparatively

underserved, offering an opportunity to civil society actors to extend their services to older audiences.

In conclusion, Switzerland's democratic resilience will depend less on the absence of threats than on the speed and coherence of its response to threats. Comparative records suggest that democracies waiting for major incidents before consolidating their counter-disinformation architecture pay a higher price than those that build such architecture in anticipation. This is especially relevant for states whose democracy depends on the integrity of democratic processes, as manifested in elections and referendums held at unusually frequent intervals; in other words, an anticipatory posture is not an option but a condition for continued democratic functioning in the 21st century.

Bibliography

- AFP France. "2 millions de voix qui 'disparaissent' pour Marine Le Pen? Une 'erreur informatique' invoque France 2." *Factuel AFP*, 25 Apr. 2022, <https://factuel.afp.com/doc.afp.com.328X87B>.
- Akers, John, et al. "Technology-Enabled Disinformation: Summary, Lessons, and Recommendations." *arXiv*, 2019, <https://doi.org/10.48550/arXiv.1812.09383>.
- Arce, Daniel. "Disinformation Strategies." *Defence and Peace Economics*, vol. 35, no. 6, 2024, pp. 659–672.
- ARCOM. "Rôle et missions de l'Arcom." *ARCOM*, <https://www.arcom.fr/assistance/faq/role-missions>.
- Arcos, Rubén, et al. *Routledge Handbook of Disinformation and National Security*. 1st ed., Routledge, 2023, <https://doi.org/10.4324/9781003190363>.
- Baumann, Fabian, et al. "Dynamics of Algorithmic Content Amplification on TikTok." *EPJ Data Science*, vol. 15, no. 1, 2026, p. 18, <https://doi.org/10.1140/epjds/s13688-026-00629-2>.
- Baumann, Mirjam, and Edda Humprecht. "Examining the Spread of Disinformation on Facebook during the First Wave of the Covid-19 Pandemic: A Case Study in Switzerland." *Communications*, vol. 50, no. 2, 2025, pp. 415–437, <https://doi.org/10.1515/commun-2023-0059>.
- Bernhard, Laurent. "The 2023 Swiss Federal Elections: The Radical Right Did It Again." *West European Politics*, vol. 47, no. 6, 2024, pp. 1435–1445, <https://doi.org/10.1080/01402382.2024.2303277>.
- Bontcheva, Kalina. *Generative AI and Disinformation: Recent Advances, Challenges, and Opportunities*.

- Bontridder, Noémi, and Yves Poulet. "The Role of Artificial Intelligence in Disinformation." *Data & Policy*, vol. 3, 2021, p. e32,
<https://doi.org/10.1017/dap.2021.20>.
- Bundesamt für Statistik BFS. *In der KI-begeisterten Schweiz nimmt Desinformation zu*. 2025,
<https://www.bfs.admin.ch/bfs/de/home/aktuell/neue-veroeffentlichungen.assetdetail.36304417.html>.
- Bundesamt für Verfassungsschutz. "Gefährdung der Bundestagswahl durch unzulässige ausländische Einflussnahme." N.d.,
<https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrung-der-bundestagswahl-2025-durch-unzulaessige-auslaendische-einflussnahme.html>.
- Bundesregierung, Die. "Bundestagswahl 2025." 2025,
<https://www.bundeswahlleiterin.de/bundestagswahlen/2025/ergebnisse/bund-99.html>.
- Bundesregierung, Die. "Regierungsbildung 2025: Koalitionsvertrag zwischen CDU, CSU und SPD." 2025,
<https://www.bundesregierung.de/breg-de/aktuelles/koalitionsvertrag-2025-2340970>.
- Bundeswahlleiter. "Fakten gegen Desinformation: Die Bundestagswahl 2021." 2021.
- Burnell, Peter, and Peter Calvert. "The Resilience of Democracy: An Introduction." *Democratization*, vol. 6, no. 1, 1999, pp. 1–32,
<https://doi.org/10.1080/13510349908403594>.
- Chatignoux, Edouard, et al. "The 2015 and 2016 Terrorist Attacks in France: Was There a Short-Term Impact on Hospitalizations for Cardiovascular Disease?"

Clinical Epidemiology, vol. 10, 13 Apr. 2018, pp. 413–419,

<https://doi.org/10.2147/CLEP.S154492>.

Confavreux, Pascal. "The French Response Account: A Tool for France in the

Information War." *France Diplomacy*, 5 Feb. 2026,

<https://uk.diplomatie.gouv.fr/en/french-response-account-tool-france-information-war>.

Cull, Nicholas J., et al. *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It*. 2017.

Deutscher Bundestag. "Schutz der Bundestagswahl 2021 vor Desinformation und Cyberangriffen." 2021,

<https://dibundestag.de/vorgang/schutz-der-bundestagswahl-2021-vor-desinformation-und-cyberangriffen/276848>.

Digital Forensic Research Lab. "The French Election through Kremlin Eyes: How the Russian State's French-Language Wire Portrays the French Election."

DFRLab, 20 Apr. 2017,

<https://medium.com/dfrlab/electionwatch-scottish-vote-pro-kremlin-trolls-f3cca45045bb>.

Direction interministérielle de la transformation publique. (2025, September).

Information manipulation How can we understand them and better combat them?

Diossy, Nikoleta, et al. "Building Resilience Against Election Influence Operations:

Preparing for the European Elections in 2024 and Beyond." *The International Foundation for Electoral Systems*, Apr. 2024,

<https://www.ifes.org/publications/building-resilience-against-election-influence-operations>.

European Commission. *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence*. Feb. 2023,
https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

European Commission. *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations*. 2025,
https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en.

European Commission. *4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards*. Policy Planning and Strategic Communication, 2026.

European Commission. *Code of Practice on Disinformation*. 2022.

European Commission. "Commission Services Sign Administrative Arrangements with French and Irish Media Regulators to Support Enforcement of Digital Services Act." Press release, 23 Oct. 2023,
https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_5196/IP_23_5196_EN.pdf.

European Commission. "Democracy." *Directorate-General for International Partnerships*,
https://international-partnerships.ec.europa.eu/policies/peace-and-governance/democracy_en.

EUvsDisinfo. "Tackling Disinformation à la Française." *EUvsDisinfo*, 2 Apr. 2019,
<https://euvsdisinfo.eu/tackling-disinformation-a-la-francaise/>.

EUvsDisinfo. "Vilifying Germany, Wooing Germany." *EUvsDisinfo*, 9 Mar. 2021, <https://archive.ph/3PQpc>.

Factuel AFP. "Non, la 'société Dominion' n'a pas été mandatée pour 'compiler les résultats de l'élection 2022.'" *Factuel AFP*, 25 Mar. 2022, <https://factuel.afp.com/doc.afp.com.326N6U9>.

Faris, Robert, et al. *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election*. Berkman Klein Center for Internet & Society, 2016.

Federal Council. *Influence Activities and Disinformation: Report of the Federal Council*. 22.3006, 2024, <https://www.sepos.admin.ch/en/influencing-activities-disinformation>.

Federal Council. *The Security Policy of Switzerland: Report of the Federal Council*. 21.070, 2021, <https://www.sepos.admin.ch/en/security-policy-report-2021>.

Federal Department of the Environment, Transport, Energy and Communications DETEC. (2025, October 29). New law on communication platforms and search engines: Start of consultation proceedings [Press Release]. Schweizer Eidgenossenschaft. <https://www.uvek.admin.ch/en/newnsb/6TmEAde4htulaWG9CWYtK>

Federal Foreign Office. *Technical Report on an Analysis by the Federal Foreign Office, Germany Targeted by the Pro-Russian Disinformation Campaign "Doppelgänger"*. 2024, <https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf>.

- Federal Government Germany. *Was ist Desinformation?* 2026,
<https://www.bundesregierung.de/breg-de/aktuelles/was-ist-desinformation-1875148>.
- Federal Government Germany, Federal Ministry of the Interior and Community.
Working Together to Combat Manipulation: Protecting the 2025 Bundestag Elections from Hybrid Threats, Including Disinformation. 2024,
https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2025/BM125014-zusammen-gg-manipulation_englisch.pdf.
- Federal Intelligence Service FIS. *Situation Report of the Federal Intelligence Service* 2024. 2024, <https://www.admin.ch/en/nsb?id=102858>.
- Federal Intelligence Service FIS. *Switzerland's Security 2023: Situation Report of the Federal Intelligence Service.* 2023,
<https://www.news.admin.ch/en/nsb?id=95984>.
- Federal Ministry of Interior and Community. "Bundestagswahl 2021 – Mögliche illegitime Einflussversuche fremder Staaten: Fragen und Antworten." 2021,
<https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/08/sicherheit-bundestagswahl.pdf>.
- Ferrara, Emilio. "The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth." *arXiv*, 1 Jan. 2026, <https://doi.org/10.48550/arXiv.2601.00306>.
- Feuerriegel, Stefan, et al. "Research Can Help to Tackle AI-Generated Disinformation." *Nature Human Behaviour*, vol. 7, no. 11, 2023, pp. 1818–1821, <https://doi.org/10.1038/s41562-023-01726-2>.
- fög. *Jahrbuch Qualität der Medien*. Research Center for the Public Sphere and Society, 2025, <https://doi.org/10.24894/978-3-7965-5366>.

"France's 2017 Presidential Election: In Brief." *Congressional Research Service*, 28

Apr. 2017,

https://www.everycrsreport.com/files/20170428_R44815_742b640592c5ba1dfd568cdbfa59c1efd9558d1a.pdf.

"France: Freedom in the World 2020 Country Report." *Freedom House*, 2019,

<https://freedomhouse.org/country/france/freedom-world/2020>.

"French Military to Boost Cyber Defence in Wake of Hacking Scandals." *France 24*,

1 Aug. 2017,

<https://www.france24.com/en/20170108-french-military-boost-cyber-defence-hacking-scandals-le-drian-digital-soldiers>.

Gallo, Nathan. "Non, 22 500 gilets jaunes n'ont pas été privés de leur droit de vote."

Factuel AFP, 21 Apr. 2022, <https://factuel.afp.com/doc.afp.com.328L927>.

Germano, Fabrizio, et al. *Ranking for Engagement: How Social Media Algorithms Fuel Misinformation and Polarization*.

GUILLAUME, M. (n.d.). Combating the manipulation of information – a French case

(Hybrid CoE Strategic Analysis 16). Hybrid CoE. Retrieved

https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_16_manipulation-of-information_.pdf

Grub, Maria F. *Defining the Role(s) of AI in Disinformation Research: A Systematic Review*. 2025.

Ha, Louisa, et al. "Mapping Recent Development in Scholarship on Fake News and Misinformation, 2008 to 2017: Disciplinary Contribution, Topics, and Impact." *American Behavioral Scientist*, vol. 65, no. 2, 2021, pp. 290–315.

Hastuti, Hastuti, et al. "Algorithmic Influence and Media Legitimacy: A Systematic Review of Social Media's Impact on News Production." *Frontiers in*

Communication, vol. 10, 2025, p. 1667471,
<https://doi.org/10.3389/fcomm.2025.1667471>.

Hénin, Nicolas. *Disinformation Landscape in France*. EU DisinfoLab, Mar. 2023,
https://www.disinfo.eu/wp-content/uploads/2023/03/20230224_FR_DisinfoFS.pdf.

Hénin, Nicolas. "Securing Information Integrity in the Upcoming French Presidential Election: A Catalogue of Initiatives." *EU DisinfoLab*, 8 Apr. 2022,
<https://www.disinfo.eu/publications/securing-information-integrity-in-the-upcoming-french-presidential-election/>.

Hénin, Nicolas. "What Did Disinformation Look Like during the 2022 French Presidential Election? An Overview Based on Fact-Checking Articles." *EU DisinfoLab*, 22 June 2022,
<https://www.disinfo.eu/publications/what-did-disinformation-look-like-during-the-2022-french-presidential-election-an-overview-based-on-fact-checking-articles/>.

Hewlett, Nick, and Raymond Kuhn. "Reflections on the 2022 Elections in France." *Modern & Contemporary France*, vol. 30, no. 2, 2022, pp. 393–409,
<https://doi.org/10.1080/09639489.2022.2134325>.

Humprecht, Edda, et al. "Resilience to Online Disinformation: A Framework for Cross-National Comparative Research." *The International Journal of Press/Politics*, vol. 25, no. 3, 2020, pp. 493–516,
<https://doi.org/10.1177/1940161219900126>.

Humprecht, Edda, et al. "The Sharing of Disinformation in Cross-National Comparison: Analyzing Patterns of Resilience." *Information, Communication*

& *Society*, vol. 26, no. 7, 2023, pp. 1342–1362,

<https://doi.org/10.1080/1369118X.2021.2006744>.

Institute for Strategic Dialogue. "FIMI Response Team Report — Country Report:

Assessment of Foreign Information Manipulation and Interference (FIMI) in the 2025 German Federal Election." 2026,

<https://www.isdglobal.org/publication/country-report-assessment-of-foreign-information-manipulation-and-interference-fimi-in-the-2025-german-federal-election/>.

Jonah, Anaëlle. "From Soft Power to Digital Firepower: France Steps Up Fight

against Disinformation." *France 24*, 9 Aug. 2025,

<https://www.france24.com/en/france/20250908-from-soft-power-to-digital-firepower-france-steps-up-against-online-disinformation-french-response>.

Kondratov, Eugene, and Elisabeth Johansson-Nogués. "Russia's Hybrid Interference

Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal Democracies?" *Geopolitics*, Nov. 2022,

<https://doi.org/10.1080/14650045.2022.2129012>.

Kupiecki, Robert, et al. *International Disinformation: A Handbook for Analysis and*

Response. Brill, 2025, <https://doi.org/10.1163/9789004715769>.

Le Journal du Dimanche. "Le Drian sur le cyberespionnage: 'La France n'est pas à

l'abri, il ne faut pas être naïf.'" *Le Journal du Dimanche*, 7 Jan. 2017,

<https://www.lejdd.fr/International/Le-Drian-sur-le-cyberespionnage-La-France-n-est-pas-a-l-abri-il-ne-faut-pas-etre-naif-837985>.

Legendre, Anne-Claire. "France's 'Diplomacy of Combat' Means 'Countering

Disinformation,' Spokeswoman Says." *France 24*, 6 Sept. 2022,

<https://www.youtube.com/watch?v=EBi8jIdXxxk>.

- Lorenz-Spreen, Philipp, et al. "A Systematic Review of Worldwide Causal and Correlational Evidence on Digital Media and Democracy." *Nature Human Behaviour*, vol. 7, no. 1, 2022, pp. 74–101, <https://doi.org/10.1038/s41562-022-01460-1>.
- Marchant de Abreu, Catalina. "Doppelgänger: France Accuses Russia of Usurping News Websites in Disinformation Campaign." *France 24*, <https://www.france24.com/en/tv-shows/truth-or-fake/20230614-doppelgänger-france-accuses-russia-of-usurping-main-media-websites-in-disinformation-campaign>.
- Marwick, Alice, and Rebecca Lewis. *Media Manipulation and Disinformation Online*. Data & Society Research Institute, 15 May 2017, <https://datasociety.net/library/media-manipulation-and-disinfo-online/>.
- Merkel, Wolfgang. "What Is Democratic Resilience?" *Democratization*, 2025, pp. 1–22, <https://doi.org/10.1080/13510347.2025.2590677>.
- Milli, Smitha, et al. "Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media." *PNAS Nexus*, vol. 4, no. 3, 2025, p. pgaf062, <https://doi.org/10.1093/pnasnexus/pgaf062>.
- Ministère des Armées. (2025, March 1). Disinformation, a weapon of war. <https://www.defense.gouv.fr/en/news/disinformation-weapon-war>
- Morosoli, Sophie, et al. "Identifying the Drivers Behind the Dissemination of Online Misinformation: A Study on Political Attitudes and Individual Characteristics in the Context of Engaging with Misinformation on Social Media." *American Behavioral Scientist*, vol. 69, no. 2, 2025, pp. 148–167, <https://doi.org/10.1177/00027642221118300>.

- NATO. *NATO's Approach to Counter Information Threats*. 3 Feb. 2025,
<https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats>.
- Newman, Nic, et al. *Reuters Institute Digital News Report 2025*. Reuters Institute for the Study of Journalism, 2025, <https://doi.org/10.60625/RISJ-8QQF-JT36>.
- North, Daria Azariev, et al. *Building Resilience Against Election Influence Operations: Preparing for the European Elections in 2024 and Beyond*. International Foundation for Electoral Systems, 2024,
<https://www.ifes.org/publications/building-resilience-against-election-influence-operations>.
- OECD. *OECD Survey on Drivers of Trust in Public Institutions — 2024 Results*. OECD Publishing, 2024,
https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_9a20554b-en.html.
- Paul, Christopher, and Miriam Matthews. *The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It*. RAND Corporation, 2016, <https://doi.org/10.7249/PE198>.
- "Piratage d'En Marche!: Les hackers ont trouvé la faille." *Public Sénat*, 6 May 2017,
<https://www.publicsenat.fr/actualites/politique/piratage-d-en-marche-les-hackers-ont-trouve-la-faille-60159>.
- Rensmann, Lars, and Thijs de Zee. "The Pandemic Factor: The COVID-19 Crisis in the Alternative for Germany's 2021 Federal Election Campaign." *German Politics & Society*, vol. 40, no. 4, 2022, pp. 69–103,
<https://doi.org/10.3167/gps.2022.400404>.

- Romanishyn, Alexander, et al. "AI-Driven Disinformation: Policy Recommendations for Democratic Resilience." *Frontiers in Artificial Intelligence*, vol. 8, 2025, p. 1569115, <https://doi.org/10.3389/frai.2025.1569115>.
- Scharfbillig, Mario, et al. Fractured Reality. European Commission, Joint Research Centre, 2026. DOI.org (CSL JSON), <https://data.europa.eu/doi/10.2760/9358883>.
- Serrano, Raquel Miguel, and EU DisinfoLab. "Disinformation Landscape in Germany." 2023, https://www.disinfo.eu/wp-content/uploads/2023/03/20230224_GER_DisinfoFS.pdf.
- Severson, Daniel. "France's Extended State of Emergency: What New Powers Did the Government Get?" *Lawfare*, 22 Nov. 2015, <https://www.lawfaremedia.org/article/frances-extended-state-emergency-what-new-powers-did-government-get>.
- SGDSN. *RRN: A Complex and Persistent Information Manipulation Campaign*. SGDSN, 19 July 2023, https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf.
- SGDSN. (2022, November 17). Service for monitoring and protection against foreign digital interference. General secretariat for Defence and National Security. <https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques>
- SGDSN. "Service de vigilance et protection contre les ingérences numériques étrangères." *SGDSN*,

<https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques>.

Sikora, Krysia, et al. "Europe's Other Battlefields: Foreign Hybrid Threats in the EU."

Institute for Strategic Dialogue, 2026,

<https://www.isdglobal.org/wp-content/uploads/2026/02/Foreign-Hybrid-Threats-in-the-EU.pdf>.

Simchon, Almog, et al. "The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence." *PNAS Nexus*, vol. 3, no. 2, 2024, p.

pgae035, <https://doi.org/10.1093/pnasnexus/pgae035>.

Strasser, Matthias. "Mitte-Links-Allianz: Keine Deepfakes im Wahlkampf." *SRF*, 25 Sept. 2023,

<https://www.srf.ch/news/schweiz/wahlen-2023/regulierung-von-ki-mitte-links-allianz-keine-deepfakes-im-wahlkampf>.

Thouvenin, Florent, et al. "Governance von Desinformation in digitalisierten Öffentlichkeiten." *Jusletter*, 5 Feb. 2024.

Vaccari, Cristian, and Andrew Chadwick. "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media + Society*, vol. 6, no. 1, Jan. 2020,

<https://doi.org/10.1177/2056305120903408>.

Van Der Linden, Sander, et al. "Prebunking Misinformation Techniques in Social Media Feeds: Results from an Instagram Field Study." *Harvard Kennedy School Misinformation Review*, 22 Jan. 2026,

<https://doi.org/10.37016/mr-2020-193>.

Vilmer, Jean-Baptiste Jeangène, et al. "Lessons from the Macron Leaks." *Hacks*,

Leaks and Disruptions: Russian Cyber Strategies, edited by Nicu Popescu and

Stanislav Secieru, European Union Institute for Security Studies (EUISS),
2018, pp. 75–84. *JSTOR*, <http://www.jstor.org/stable/resrep21140.11>.

Viginum. (2021). Défis et opportunités de l'intelligence artificielle dans la lutte contre les manipulations de l'information.

https://doi.org/https://www.sgdsn.gouv.fr/files/files/Publications/20250207_N_P_SGDSN_VIGINUM_Rapport%20menace%20informationnelle%20IA_VF.pdf

Vogler, Daniel, et al. *Falschinformationen, Alternativmedien und Verschwörungstheorien: Wie die Schweizer Bevölkerung mit Desinformation umgeht*. Bericht für das Bundesamt für Kommunikation, Forschungszentrum Öffentlichkeit und Gesellschaft (fög), University of Zurich, 2021,
<https://doi.org/10.5167/UZH-219206>.

Wardle, Claire, and Hossein Derakhshan. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking*. Council of Europe, 2017.

List of Figures

Fig. 1: *Case Study Procedure by Yin*. Yin, Robert K. *Case Study Research. Design and Methods*. 5th edition. Los Angeles: Sage, 2014. Web.

Fig. 2: *Trends in the Context of Global Digital Dynamics (2019–2025)*. Romanishyn, Alexander, et al. «AI-Driven Disinformation: Policy Recommendations for Democratic Resilience». *Frontiers in Artificial Intelligence*, vol. 8, p. 1569115. DOI.org (Crossref), <https://doi.org/10.3389/frai.2025.1569115>.

Fig. 3: *Distribution of Seats in the Bundestag. 2025 Compared to 2021.* Federal Returning Officer. *Bundestag election 2025, 2025.*
<https://www.bundeswahlleiterin.de/en/bundestagswahlen/2025/ergebnisse/bund-99.html>

Fig. 4: *Automated Content Distribution Systems.* Federal Foreign Office. *Technical Report on an Analysis by the Federal Foreign Office, Germany Targeted by the Pro-Russian Disinformation Campaign “Doppelgänger”, 2024.*
<https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf>