

TOOLKIT for participation and critical thinking



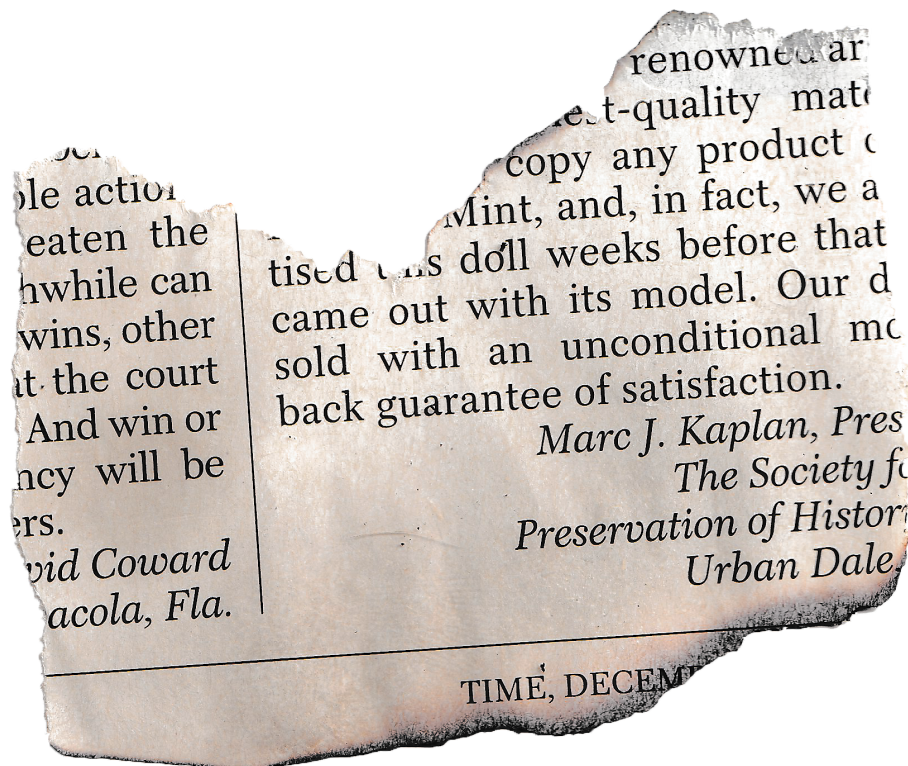
DEMOCRACY ● MEDIA LITERACY ● RESILIENCE ●



Co-funded by
the European Union

DEMOCRACYWISE TOOLKIT

Our actions for citizens' participation and critical thinking





**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of Contents

DISINFORMATION, MISINFORMATION AND FIMI

Building Civic Resilience – The Strategy of Pre-bunking

Eroding Trust

Civil Society Needs

Tools

Activities



Part 1: DISINFORMATION, MISINFORMATION AND FIMI

What, why and where

This introduction provides a comprehensive overview of the information manipulation landscape, defining key concepts and categorizing the threats we face in the digital age.



What is Disinformation?

Disinformation is the intentional creation, presentation, and dissemination of false, inaccurate, or misleading information designed to cause public harm or generate profit. It is a critical component of what experts call "information disorder," an ecosystem where ideologies, emotions, and algorithms converge to polarize public opinion. It must be clearly distinguished from misinformation, which is the sharing of false information in good faith, where the individual believes the content is true and lacks a deliberate intent to deceive.



To understand why disinformation is so effective, we must look at the psychological and technological mechanisms it exploits:

- **Psychological Levers and Cognitive Biases:** disinformation is strategically crafted to bypass critical thinking. It leverages the "confirmation bias," our tendency to believe information that confirms our pre-existing worldviews, and the use of "heuristics," mental shortcuts that allow us to judge the truth of a claim quickly without deep analysis. Furthermore, content that triggers strong emotions—such as fear, outrage, or a sense of group belonging—is significantly more likely to be shared and internalized than purely logical data.
- **"Augmented disinformation" via AI:** the integration of Artificial Intelligence (AI) has transformed disinformation from a manual process into a high-speed, automated weapon. Generative AI enables the mass production of synthetic media, including deepfakes (manipulated audio, video, or images that appear authentic) and highly persuasive text generated by Large Language Models (LLMs). These technologies create an "epistemic threat," making it nearly impossible for citizens to distinguish reality from fabrication, which leads to the "liar's dividend"—a phenomenon where public figures can deny real evidence by claiming it is a digital manipulation.
- **Micro-targeting and behavioral manipulation:** digital platforms use AI to collect behavioral, demographic, and psychometric data, allowing threat actors to engage in micro-targeting. This means a disinformation narrative can be personalized for a specific individual, exploiting their unique fears and cognitive biases to make the manipulation more persuasive and credible.
- **A strategic tool of foreign policy:** in the context of Foreign Information Manipulation and Interference (FIMI), disinformation is not a sporadic occurrence but a strategic instrument of foreign policy. Actors like Russia, China and others utilize a "kill chain"—an end-to-end process of planning, preparing, and executing attacks—to saturate the information space. They often employ Coordinated Inauthentic Behavior (CIB), using networks of bots and "troll farms" to simulate a false sense of widespread public consensus, thereby eroding trust in democratic institutions and the international rules-based order.

Kinds of disinformation online

The disinformation landscape is highly diverse, with threats categorised both by the strategic objectives they pursue and the technical formats they employ to deceive the public.

1. Strategic objectives and targets

Disinformation is rarely a series of isolated incidents; it is often part of a coordinated campaign with specific goals, particularly during sensitive periods like elections:

- Targeting information consumption: threat actors attempt to control the flow of information and set the agenda on key topics. This is often done by establishing infrastructure (like proxy media or social media channels) well in advance to prime audiences with specific narratives.

- Targeting candidates and political parties: this involves direct personal attacks to undermine reputations, such as allegations of corruption or scandals. One notable method is the use of "hack-and-leak" operations, where private information is stolen via cyber-attacks and then amplified through manipulative narratives to discredit targets.

- Targeting trust in democracy: campaigns portray electoral systems as weak, fraudulent, or open to manipulation. This includes spreading false allegations of voting irregularities to discourage participation and delegitimise results.

- Targeting polarization (identity-based disinformation): disinformation is frequently used to exploit social divisions by targeting specific groups based on their identity, such as the LGBTIQ+ community, ethnic minorities, or women.

- Targeting citizens' ability to vote: actors may attempt to suppress the vote by spreading false information about polling station security (e.g., fake bomb threats) or misleading citizens about voting requirements and procedures.

2. Tactical formats and distribution

The "how" of disinformation relies on a variety of tactics designed to increase the perceived legitimacy of false content:

- Synthetic media and deepfakes: the use of Artificial Intelligence (AI) to create realistic but fabricated audio, images, or videos. This

includes "face swapping" public figures or using AI-generated voices to make them appear to say things they never did.

- Decontextualized content: one of the most common tactics is the repurposing of genuine content—such as old videos or images—presented in a new, misleading context to support a false claim.

- Impersonation and clone sites: threat actors create clones of legitimate news outlets (like the BBC or Der Spiegel) or official government websites to lend credibility to their disinformation.

- Coordinated inauthentic behavior (CIB): this is the use of networks of fake accounts, bots, and "troll farms" to simulate a false sense of widespread public consensus.

- Cross-platform coordination: content is rarely confined to one site; it is strategically seeded and amplified across multiple platforms (e.g., Telegram, X, and Facebook) simultaneously to maximize reach and hide the original source of the manipulation.

While the formats used to create content are evolving with AI, the manipulative behavior—the coordinated effort to bypass critical thinking through emotional resonance and inorganic amplification—remains the defining characteristic of modern disinformation online.

Foreign Information Manipulation and Interference (FIMI)

Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures, and political processes. This activity is manipulative in character and is conducted in an intentional, strategic, and coordinated manner by state or non-state actors, including their proxies. Unlike general disinformation, FIMI is not a sporadic opportunity but a strategic instrument of foreign policy and a crucial component of modern-day warfare.

1. Key Actors and Strategic Styles

While many actors engage in FIMI, Russia and China are the most prominent state actors identified in the sources. They often employ distinct styles:

- Russia: typically uses a "quantity-over-quality" strategy, producing

massive amounts of content across hundreds of channels to saturate the information space and create confusion. These operations are integrated across diplomatic networks, security services, state-controlled media (like RT and Sputnik), and "troll farms".

-China: generally adopts a more subtle and institutionalized approach. It uses official state media (like CGTN and China Daily) and opaque channels to build a presence in the global information space, improve its international image, and suppress critical voices.

2. Tactical Characteristics: how FIMI works

FIMI actors use a variety of tactics, techniques, and procedures to achieve their goals. Common characteristics include:

-Coordinated inauthentic behavior (CIB): this involves the use of networks of fake accounts, bots, and professional troll farms to simulate a false sense of widespread, spontaneous consensus.

-Cross-platform coordination: this is the default modus operandi; threat actors seed and amplify content across multiple social media platforms (such as Telegram, X, and Facebook) and websites simultaneously to obfuscate the original source and maximize reach.

-Targeting diversity: FIMI targets countries (Ukraine remains the primary target), international organizations like the EU and NATO, and individuals, including politicians and celebrities. It also exploits existing divisions by targeting specific groups, such as the LGBTQ+ community.

-Events as catalysts: FIMI activity often seizes on the attention surrounding significant events, such as elections, political summits, or crises, to hijack the narrative.

3. The EU FIMI Toolbox: A Multi-Level Response

To counter these threats, the EU has developed the FIMI Toolbox, a comprehensive set of instruments organized into four pillars:

1. Situational awareness: systematic monitoring and detection to understand threat actors and their TTPs.
2. Resilience building: strengthening society through strategic communications, media literacy, and support for independent media and civil society.
3. Disruption and regulation: implementing legislative frameworks like the Digital Services Act (DSA) and the AI Act to ensure

transparency and accountability on digital platforms.

4. External action and diplomatic response: utilizing foreign policy tools, such as international cooperation (G7, NATO), political attribution, and sanctions against malign actors.

4. The response framework: from analysis to action

The FIMI Response Framework provides a structured approach for stakeholders to prevent, react to, and adapt to attacks:

- Pre-incident (Prevent): establishing common methodologies and building long-term societal resilience.

- Mid-incident (React): activating reactive countermeasures to contain (e.g., pre-bunking), minimize (e.g., removing content), or redirect (e.g., exposing the actor) the spread of an incident.

- Post-incident (Adapt): evaluating the impact, sharing lessons learned, and implementing deterrence measures like legal responses or sanctions.

Ultimately, because FIMI is a networked threat, the response must also be networked, involving a "whole-of-society" approach that connects governments, the private sector, civil society, and independent media.

Part 2: Building Civic Resilience – The Strategy of Pre-bunking

Prevent and react to disinformation

This chapter explores how democratic societies can defend themselves against disinformation and Foreign Information Manipulation and Interference (FIMI) by fostering **civic resilience**. Rather than relying solely on reactive measures like fact-checking, this approach emphasizes proactive strategies that prepare citizens to recognize and resist manipulative tactics before they take root.

Understanding digital social resilience

Resilience is the capacity of communities to cope with, adapt to, and withstand external stresses—such as disinformation and FIMI—by mobilizing transformative capacities to sustain societal well-being. In the digital context, digital social resilience is defined as the ability of individuals and groups to leverage online environments to maintain social capital, cohesion, and collective efficacy.

To build an effective toolbox, it is necessary to distinguish between two interconnected layers:

- The individual layer (digital literacy): digital literacy encompasses the technical and cognitive skills needed to navigate the internet. While it serves as a foundational skill, literacy alone does not automatically translate into resilience. Literacy becomes protective when it is activated before exposure to threats and supported by a broader social context.

- The community layer (social infrastructure): true resilience is not just a technical skill; it is a social process. It depends on collective verification practices embedded within communities. This is the "meso-level mechanism" of defense, where community networks transform individual digital literacy into collective resilience through trusted intermediaries.

Key mechanisms of social resilience:

- Collective social correction: this refers to the ongoing practice of verifying and correcting information within group contexts. In these networks, members pool their knowledge, exercise collective judgment, and co-construct shared standards for information sharing.

- Trusted intermediaries: Civil Society Organizations (CSOs) and local community groups are essential nodes in this infrastructure. They are often perceived as more credible than authorities or traditional media, allowing them to reach underserved or vulnerable audiences that are frequent targets of FIMI.

- Intergenerational knowledge exchange: resilience is strengthened when different generations collaborate; for instance, younger users provide technical fluency while older users contribute contextual knowledge and experience with information evaluation.

A Whole-of-Society Approach

Building social resilience requires a "whole-of-society" approach. This means moving beyond individualistic Western models of skill acquisition toward a model of community empowerment. By integrating formal pre-bunking strategies into existing community infrastructures, societies can embed collective verification routines into daily information use, creating a "mental vaccine" that protects the common public space.

Pre-bunking: the mental “vaccine”

Pre-bunking (or preemptive debunking) is a proactive defense strategy designed to build psychological resistance against disinformation and FIMI before an individual is even exposed to it. While traditional fact-checking is a reactive "cure" that often struggles to keep pace with the viral spread of falsehoods, pre-bunking acts as a prophylactic measure.

The Inoculation Analogy

This strategy is conceptually grounded in Inoculation Theory, developed by social psychologist William J. McGuire in the 1960s. It follows a medical vaccination metaphor: just as a biological vaccine exposes the body to a weakened version of a virus to trigger an immune response, attitudinal inoculation exposes people to a "weakened dose" of a manipulative tactic or misinformation. This "microdose" is strong enough to alert the mind to the threat but not so convincing as to deceive the person, thereby training their "mental antibodies" to recognize and reject similar attacks in the future.

To be effective, pre-bunking interventions typically follow a structured three-step process:

- Emotional warning: an explicit alert that threat actors are attempting to manipulate the audience. This creates a sense of "threat," which provides the necessary motivation for individuals to protect their existing beliefs.
- The microdose: providing a harmless, often exaggerated or humorous, example of a manipulative technique—such as deepfakes, impersonation, or emotional baiting.
- Refutational pre-emption: equipping the audience with the specific

cognitive tools and counterarguments needed to deconstruct and spot the manipulation technique.

DEMOCRACYWISE experience has shown that active experiential learning is one of the most effective ways to "inoculate" a population. Rather than passively receiving information, citizens are encouraged to "step into the shoes" of a manipulator through educational games and simulations. The project made a review of the most popular projects that use this technique:

- "Bad News": a game where players learn to use six common manipulation techniques (trolling, polarization, impersonation, conspiracy, emotion, and discrediting) to gain followers in a simulated environment.

- "Under Pressure": a serious game designed for students to practice spreading disinformation in a protected environment, kickstarting critical conversations about digital citizenship.

- Community-based initiatives: programs like Indonesia's "Tular Nalar" or Ireland's "Be Media Smart" leverage local networks and civil society to translate these psychological frameworks into culturally resonant everyday practices.

By focusing on the manipulative behaviors and techniques rather than just specific false facts, pre-bunking offers a scalable and "broad-spectrum" defense that remains effective even as narratives change. It empowers citizens with agency, shifting them from passive consumers of information to active guardians of the digital public square.



Digital Literacy and Active Learning

Digital literacy serves as the essential foundational layer for effective pre-bunking and broader information integrity.

While pre-bunking provides the anticipatory framework for recognizing manipulation, digital literacy supplies the technical skills and critical thinking capabilities needed to apply these frameworks across different platforms and contexts. Despite its importance, significant gaps remain; for instance, European studies indicate that 43% of 14-year-olds do not reach the basic level of digital skills.

Core competencies for resilience

To build a resilient society, digital literacy must evolve beyond basic technical proficiency toward **civic-critical media literacy**. Key competencies identified as essential for modern digital citizenship include:

- Identifying facts from falsehoods: developing the ability to distinguish verifiable factual claims from subjective opinions or deceptive content;
- Lateral Reading: training users to leave a suspicious site to investigate the source's credibility through multiple other tabs and sources—a practice that is more effective than deep-diving into the suspicious site itself;
- Algorithmic awareness: understanding how platform ranking, recommendation systems, and "echo chambers" influence what information is visible and how it is shared;
- Source evaluation and triangulation: systematically scrutinizing headlines, links, and provenance to identify patterns of manipulation.

Active Learning and "Serious Games"

One of the most innovative and effective approaches to fostering digital literacy is active experiential learning. Rather than passively receiving information, participants are encouraged to "walk in the

shoes" of a manipulator through educational "serious games".

- Games and role plays allow participants to take on the role of a fake news creator in a protected, simulated environment;

- By attempting to spread disinformation and gain followers using techniques like impersonation, emotional baiting, and polarization, players build "mental antibodies" that help them recognize and reject these same tactics in real life;

- Because these interventions are game-based and digital, they are highly scalable, reaching millions of people worldwide across different languages and cultural settings.

Educational and Social Infrastructure: A Whole-of-Society Approach

Building digital literacy is a continuous process that requires a networked defense, integrating support across all levels of society to transform individual skills into a collective defense mechanism. This infrastructure moves beyond school-based learning to encompass a "whole-of-society" framework where governments, civil society, and families collaborate to safeguard the common public space.

1. Institutional and educational

- Teacher and school support: educators are the frontline of formal digital citizenship; under Action 7 of the Digital Education Action Plan, teachers are provided with updated guidelines (2026) and lesson plans to assess digital literacy and lead classroom discussions on deceptive content, such as generative AI, influencers, and deepfakes;

- Policy enablers: national and EU-level frameworks, such as the Digital Services Act (DSA) and the AI Act, provide the legal infrastructure necessary to ensure transparency in algorithms and the mandatory labeling of synthetic content; these laws empower the "defender community" to act against systemic risks to democracy

2. Civil society and community networks

- Civil Society Organizations (CSOs): CSOs serve as trusted intermediaries that bridge the gap between authorities and the public; they are often more credible than traditional media or governments and are essential for reaching underserved or vulnerable groups who

may be targets of FIMI;

- Community-based empowerment: resilience is most effective when embedded in existing social structures, such as women's organizations, youth associations, or neighborhood networks; these groups transform individual digital literacy into collective verification habits through routine practice and shared standards;

- Intergenerational knowledge exchange: societies are strengthened when age groups collaborate; while younger users often provide technical fluency, older generations contribute contextual knowledge and critical experience in information evaluation, creating a collaborative competence that exceeds individual capacity.

3. The private sector and media ecosystem

- Independent media and pluralism: a resilient infrastructure requires a healthy media landscape; efforts like the European Media Freedom Act ensure that citizens have access to diverse, high-quality information, which serves as a natural firewall against "news deserts" where disinformation thrives;

- Platform accountability: tech companies must cooperate with researchers and fact-checkers through frameworks like the Code of Practice on Disinformation to demonetize false narratives and implement rapid alert systems during crises or elections.

By integrating these diverse actors, digital literacy evolves from an individualistic skill acquisition model into a socially embedded resilience. This systemic approach ensures that when one node of the network is attacked, the collective infrastructure responds to contain, minimize, and redirect the threat.



Part 3: Eroding Trust

How Disinformation Distances Citizens from Institutions

Disinformation and Foreign Information Manipulation and Interference (FIMI) are not merely about spreading false facts; they are structured, strategic efforts designed to **undermine the credibility of democratic institutions**. By polluting the information environment, these activities aim to destroy the "common public space" necessary for rational debate, effectively making democracy impossible to function

The perception of a "Democratic Gap"

A primary objective of disinformation is to portray democratic systems as weak, fraudulent, or open to manipulation. Threat actors often use the following tactics to alienate citizens:

- Delegitimizing the process: narratives frequently claim that electoral systems are rigged, that outcomes are pre-agreed, or that vote-counting systems are unreliable; this fosters the belief that voting does not yield political change, creating a perceived "gap" between the will of the people and the actions of the state;
- The "Liar's Dividend": the mass production of AI-generated "synthetic media" (like deepfakes) creates an epistemic threat where citizens find it impossible to distinguish reality from fabrication; this allows public figures to deny real evidence by claiming it is a digital manipulation, further eroding the foundation of shared truth;
- The narrative of external control: especially concerning European institutions, disinformation often portrays national governments as mere puppets of "secretive outside forces" or distant bureaucrats in Brussels. For instance, post-election narratives in Spain claimed the country would follow the "wishes" of EU and NATO leaders regardless of the vote.

Disinformation acts as a powerful multiplier of social division. Rather than imposing a single alternative truth, it seeks to fragment public

discourse so that confusion becomes a strategy.

- Identity-based attacks: threat actors exploit existing societal divisions by targeting specific groups based on gender, sexual orientation, or race (e.g., targeting the **LGBTIQ+ community** or female politicians);
- Coordinated Inauthentic Behavior (CIB): using "troll farms" and bot networks, actors simulate a false sense of widespread consensus on extremist views; this artificially intensifies polarization.

The most tangible damage of this institutional distancing is seen in the degradation of the electoral process. Disinformation campaigns explicitly encourage abstention or the casting of invalid votes. This is done through "voluntary" means (persuading people that protest through non-participation is valid) or "involuntary" means (spreading false security alerts or misinformation about voting procedures). Personal attacks and "hack-and-leak" operations (like "MacronLeaks" or attacks on Polish candidates) are used to discredit individuals, discouraging them from running or being vocal on sensitive issues. The cumulative effect of distrust in official sources and the feeling of insecurity (e.g., fake bomb threats at polling stations) leads to lower voter turnout, which undermines the legitimacy of the resulting government.

Ultimately, for actors like Russia and China, these operations are a strategic instrument of foreign policy used to weaken the international rules-based order and destabilize Western societies from within.

Part 4: Civil Society Needs

Citizen Recommendations Against Disinformation

The fight against Foreign Information Manipulation and Interference (FIMI) is a complex security and societal challenge that requires a "whole-of-society" approach. While governments and international institutions provide necessary regulatory frameworks like the Digital Services Act (DSA) and the AI Act, true resilience must be built from the ground up, starting with civil society organizations (CSOs) and the citizens themselves. Based on recent evidence and community-led initiatives, the following recommendations, needs, and advice outline a path toward a more resilient digital public square.

Civil Society as the strategic partner

Civil society organizations are often **more credible than authorities** or traditional media and are uniquely positioned to reach underserved or vulnerable audiences.

- Authorities and platforms must move beyond "piecemeal" engagement. Partnerships should be integrated throughout the entire project lifecycle, from problem definition and design to implementation and evaluation;

- CSOs often lack the funding and technical expertise to address technological manipulations; there is an urgent need for consistent, non-transactional financial support to sustain long-term activities like community-based fact-checking and research;

- To effectively monitor and identify FIMI, civil society needs access to advanced technologies and platform data; programs like "Tech Soup" show that equipping frontline workers with technology is essential for identifying region-specific threats.

Citizens ask for:

- Citizens should be encouraged to practice group-based information verification; In community networks, members pool knowledge and exercise collective judgment, which is more effective than isolated fact-checking;

-Resilience is strengthened when age groups collaborate; younger users provide technical fluency, while older generations contribute contextual knowledge and critical experience in evaluating information;

-Digital literacy training must be tailored to local cultural values; for instance, using local community leaders as "trusted intermediaries" can help bridge the gap between formal information and marginalized groups.

-Citizens should be trained to recognize manipulation before exposure; pre-bunking focuses on teaching the rhetorical techniques used by manipulators—such as emotional baiting, false experts, and impersonation—rather than just debunking specific false facts.

Citizens and CSOs advise that the information ecosystem must be treated as a public good that respects human rights.

-Under the DSA, large platforms must be held accountable for algorithmic transparency; citizens have a right to know when they are being targeted by political ads or interacting with AI-generated synthetic content;

-Independent journalists and fact-checkers are frequent targets of harassment and suppression. There is a critical need for a European-wide protection system for these actors to ensure they can operate without fear of foreign or domestic intimidation;

-Pluralism is a natural firewall against disinformation. Support must be prioritized for local and independent media to ensure citizens have access to accurate, diverse information, especially in rural or underserved areas.

In summary, the goal is to move from a state of reactive suspicion to proactive resilience; by empowering civil society and embedding digital literacy into the social fabric, democratic societies can protect the "common public space" necessary for free debate and informed choice.

Recommendations

Recommendations for civic resilience and education

- Transition to proactive defense: move beyond reactive "debunking" toward "pre-bunking" strategies that build psychological resistance before exposure to threats;
- Adopt the pre-bunking model: utilize a structured three-step process: emotional warning, a "microdose" of the manipulation technique, and refutational pre-emption;
- Focus on techniques, not just facts: train citizens to recognize rhetorical methods like emotional baiting, false experts, and impersonation rather than focusing solely on specific false narratives;
- Promote lateral reading: encourage users to investigate a source's credibility by opening multiple tabs and verifying information across different sites;
- Enhance algorithmic awareness: educate citizens on how platform ranking and "echo chambers" influence the visibility of information;
- Establish collective verification: encourage "group-based information verification" where community members pool knowledge to exercise collective judgment;
- Leverage trusted intermediaries: utilize local community groups and CSOs, which are often perceived as more credible than traditional media or government authorities;
- Implement intergenerational exchange: pair younger users (for technical fluency) with older generations (for contextual knowledge and critical evaluation);
- Use "Serious Games": deploy interactive tools and non-formal methodologies to let citizens experience the manipulator's perspective in a safe environment;
- Institutionalize digital literacy: integrate formal digital citizenship training into school curricula, following frameworks like the Digital Education Action Plan;
- Support educators training: provide educators with lesson plans and updated guidelines (e.g., the 2026 guidelines) to lead classroom discussions on deepfakes and AI;
- Cultural adaptation: tailor digital literacy programs to local cultural values and use local leaders to reach marginalized groups.

Institutional and regulatory recommendations

- Enforce algorithmic transparency: use the Digital Services Act (DSA) to hold platforms accountable for how their algorithms target users;
- Mandate synthetic content labeling: require platforms to clearly label AI-generated content and deepfakes to protect shared truth;
- Protect information guardians: create a European-wide protection system for independent journalists and fact-checkers against harassment and intimidation;
- Support media pluralism: prioritize funding for local and independent media to prevent "news deserts" where disinformation thrives;
- Demonetize false narratives: require tech companies to work with fact-checkers to remove the profit motive from coordinated disinformation;
- Standardize crisis alert systems: implement rapid alert systems on platforms specifically during elections or social crises;
- Non-transactional funding for CSOs: provide consistent, long-term financial support to CSOs for community-based research and fact-checking;
- Equip frontline workers with tech: provide advanced monitoring technologies and platform data access to civil society organizations;
- Multi-level diplomatic response: utilize the "EU FIMI Toolbox" to implement sanctions against foreign actors engaged in strategic manipulation.

Strategic Insights on Polarisation and Trust

- Address the "Democratic Gap": counter narratives that portray democratic systems as rigged or fraudulent to prevent voter discouragement;
- Counter "Identity-Based" attacks: specifically protect groups like the LGBTIQ+ community, ethnic minorities, and women from targeted identity-based disinformation;
- Mitigate the "Liar's Dividend": educate the public on how figures might deny real evidence by falsely claiming it is a deepfake;
- Identify coordinated inauthentic behavior (CIB): train citizens to spot "troll farms" and bot networks that simulate a false sense of public consensus;
- Combat cross-platform coordination: monitor narratives that are strategically seeded across multiple apps (e.g., Telegram, X, Facebook) simultaneously;
- Discourage intentional abstention: counter campaigns that urge

citizens to cast invalid votes or abstain as a form of protest;

- Verify polling station security: proactively debunk false information regarding polling station safety, such as fake bomb threats;
- Neutralize "Hack-and-Leak" operations: educate the public on how stolen private information is amplified through manipulative narratives to discredit candidates;
- View information as a public good: treat the entire digital information ecosystem as a public good that must respect fundamental human rights.



Part 5: Tools

What DEMOCRACYWISE used to foster citizens' participation

The project was executed through a bottom-up and democratic approach, which prioritized non-discrimination and ensured equal accessibility for all participants across the 7 involved countries. The overarching management framework followed a "Structured Agile" methodology; this allowed the consortium to establish clear high-level deadlines while maintaining the flexibility necessary to adapt activities to the specific needs of local communities.

The core methodologies implemented during the project's lifecycle included:

- Community learning (Citizen Action): this was a central intergenerational approach where youth participants shared their digital fluency and media literacy skills with older community members;
- Non-formal and participatory techniques: these were applied during international workshops and local events to foster active engagement rather than passive listening.

Specific techniques included:

- Icebreakers & debriefing: facilitated through circle time and the use of "talking tools" to build trust within the group;
- Roundtable conversations: encouraged dynamic interaction by rotating participants across different thematic discussion tables;
- Collective storytelling: used to share practices and ideas through the narration of personal experiences.

Advisory and monitoring structures:

- Local citizens' panels: participants formed small discussion groups that produced formal reports of needs and recommendations;
- Local monitoring groups: citizens remained engaged by identifying and debunking disinformation that impacted their local democratic debates.
- Targeted outreach: the project utilized extensive local research and localized town hall meetings to involve marginalized and "hard-to-reach" groups directly in the activities.

DEMOCRACYWISE Approach:

1. Group building and interaction

These activities were essential during the Project Initiation (WP1) and International Workshops (WP3, WP4, WP6) to align participants from seven different countries.

- Icebreakers and debriefing: facilitated through "circle time" meetings using a "talking tool" to manage turn-taking and encourage open introduction;
- Team-building sessions: designed to bridge the intergenerational gap between youth (18–30) and elderly (60+) participants;
- Collective storytelling: participants shared personal experiences and practices through story-sharing to co-construct shared standards for evaluating information.

2. Participatory knowledge exchange

Used primarily during Capacity Building (WP3) and Community Engagement (WP4) to foster peer-to-peer learning.

- Roundtable conversations: participants formed small groups around specific topics, rotating periodically to connect with various subjects and diverse peers;
- Pro-active working groups: participants collaborated to devise local implementation plans and future actions for their home communities;
- Community learning (Citizen Action): younger participants shared technical fluency in digital citizenship, while older participants contributed contextual knowledge.

3. Practical skill-building and gamification

These activities were the core of the Media Literacy Campaigns (WP5) and workshops to provide hands-on experience.

- "Serious Games" simulations: utilizing tools like "Bad News" and "Under Pressure" where participants took on the role of a fake news creator to build "mental antibodies" against real manipulation;
- Case studies and hands-on verification: participants practiced with real-world examples of manipulated news using data verification platforms;
- Lateral reading training: an activity teaching participants to investigate source credibility by navigating multiple tabs and external verification sources.

4. Civic action and institutional dialogue

These activities focused on the project's long-term impact and sustainability during WP2, WP4, and WP6.

- Local Citizens' Panels: facilitated discussion groups that gathered recommendations and needs to be submitted to policy-makers and MEPs;
- Local monitoring groups: ongoing citizen activities dedicated to identifying, debating, and debunking local disinformation;
- Needs assessment: community events used to collect baseline data on knowledge and attitudes through interviews and interactive surveys;
- Closure retrospectives: evaluation sessions in Sumeg and closure meeting in Brussels to summarize outcomes and plan for the project's future legacy.

Part 6: Activities

Templates everybody can use

Activity 1 - Democracy

Objective: To empower citizens to identify barriers to participation and co-design recommendations for local and EU decision-makers.

Phase 1: Icebreaking and Team Building (30 Minutes)

- **Circle time and talking tool:** participants sit in a circle. A "talking tool" (a physical object) is passed around
- **Activity:** each participant shares a brief story of a time they felt their voice "did" or "did not" count in a community decision
- **Goal:** to build a sense of group belonging and validate diverse personal experiences.

Phase 2: Collective Storytelling (45 Minutes)

- **Intergenerational exchange:** participants are divided into small groups pairing youth (18–30) with elderly (60+) citizens.
- **Activity:** "The Evolution of Debate." Older participants describe how they participated in democracy before the digital age; younger participants describe their current digital engagement.
- **Goal:** to pool contextual knowledge and technical fluency, fostering "Citizen Action".

Phase 3: Roundtable "Problem Lab" (60 Minutes)

- **Rotating Tables:** set up three tables, each focused on a specific challenge:
 1. **Skepticism:** why do people stop trusting institutions?
 2. **Polarization:** how do echo chambers divide our local community?
 3. **Disinformation:** what "emotional baits" are currently trending in our news feeds?
- **Methodology:** groups rotate every 20 minutes to contribute ideas to each table's flipchart.
- **Goal:** to identify local specificities of systemic democratic threats.

Phase 4: Pro-active Design and Pre-bunking (60 Minutes)

- **Activity:** based on the identified disinformation threats, groups must design a "micro-dose" warning (a humorous poster or short script) that exposes the manipulation technique used in those threats;
- **Technical tool:** participants use the DemocracyWise Toolkit and lateral reading techniques to verify facts and source credibility;
- **Goal:** to move from passive consumption to pro-active resilience.

Phase 5: Recommendation Drafting (45 Minutes)

- **Citizen panel output:** each group selects their top 3 priority needs;
- **Activity:** drafting a report of recommendations addressed to local authorities;
- **Goal:** to bridge the "Democratic Gap" by creating a direct channel to policy-makers.

Phase 6: Debriefing and impact survey (15 Minutes)

- **Closing circle:** final reflections using the talking tool.

Activity 2 - Disinformation

Objective: to transform citizens from passive content consumers into proactive "Information Guardians" using psychological inoculation and intergenerational collaboration.

1. Warm-up: the Intergenerational Bridge (45 min)

- **Methodology:** community Learning (Citizen Action).
- **Activity:** participants are paired in small "Action Units" consisting of youth (18–30) and seniors (60+).
- **Task:** "The News Evolution Challenge." Seniors describe how they identified "propaganda" in the pre-internet era, while youth demonstrate current social media algorithms.
- **Goal:** to combine the technical fluency of younger generations with the contextual experience and critical skepticism of older citizens.

2. Core Activity: "The Puppet Master" Simulation (60 min)

- **Methodology:** Pre-bunking and gamification
- **Task:** participants step into the shoes of a disinformation producer. They must "earn followers" by selecting headlines that use specific manipulation techniques: emotional bait, conspiracy theories, or impersonation

- **Goal:** To vaccinate the mind by exposing citizens to weakened doses of manipulation, making them easier to spot in the wild.

3. Technical workshop: lateral reading (45 min)

- **Methodology:** Civic-Critical Media Literacy
- **Activity:** Practical verification
- **Task:** "Don't Sink—Go Lateral" Participants are given a suspicious local news story. Instead of analyzing the site itself, they must open multiple tabs to investigate the source's reputation through third-party mentions and fact-checking databases
- **Goal:** to break the habit of trusting professional-looking web design and focus on source credibility.

5. Closing and impact (15 min)

- **Activity:** Circle Time with a "Talking Tool"
- **Task:** each participant shares one "Red Flag" they will look for in their news feeds starting tomorrow
- **Verification:** completion of the EU Survey on Justice, Rights and Values to measure the session's impact on institutional trust and civic resilience.

Activity 3

Objective: To gather authentic citizen testimonies on democratic barriers and community needs by turning participants into "books" and "readers".

1. Warm-up: The "Silent Gallery" (25 min)

- **Methodology:** Visual Non-formal Education.
- **Activity:** The walls are covered with posters featuring open-ended prompts: *"I feel represented when..."*, *"Information becomes a weapon when..."*, *"Participation is hard because..."*.
- **Task:** Participants walk in silence and write their immediate thoughts on the posters using sticky notes.
- **Goal:** To capture raw, unfiltered "baseline data" before social influence takes over.

2. Deep Dive: "The Human Bookshelf" (60 min)

- **Methodology:** Collective Storytelling and Intergenerational Exchange.
- **Activity:** Participants are divided into "Books" (storytellers) and "Readers" (listeners).
- **Task:** "Books" share a 5-minute personal account of a democratic challenge they faced (e.g., encountering a fake news story that

- caused local panic or feeling ignored by local council).
- **Intergenerational Twist:** A senior "Book" might share a story of traditional civic engagement, while a youth "Reader" interprets how that story translates to today's digital world.
- **Goal:** To humanize qualitative data and build empathy across demographic divides.

3. The "Synthesis Lab" Roundtables (50 min)

- **Methodology:** Roundtable Conversations and Pro-active Groups.
- **Activity:** Based on the "Human Library" stories, participants move to tables categorized by **Impact Levels**:
 - **Table 1: Local Neighborhood Impact** (e.g., community trust).
 - **Table 2: National Identity & Debate** (e.g., election integrity).
 - **Table 3: European Citizenship** (e.g., EU-wide media standards).
- **Task:** Every 15 minutes, groups rotate to add "Evidence" (stories heard) and "Solutions" (ideas) to a communal canvas.
- **Goal:** To categorize individual voices into structured thematic data for the **Local Citizens' Panels**.

4. Direct Action: "The Video Message Booth" (45 min)

- **Methodology:** Community Action and Digital Engagement.
- **Activity:** Setting up a semi-private "recording corner".
- **Task:** Participants record a 60-second message addressed to their local MEP or decision-maker, starting with the phrase: "As a citizen of [City/Country], I want you to know that...".
- **Goal:** To provide a multi-modal way of gathering voices that feels more personal and urgent than a written report.

5. Closing: The "Circle of Commitment" (20 min)

- **Methodology:** Circle Time and Debriefing.
- **Activity:** A final circle where the "talking tool" is used to share one thing they learned from a "Book" that wasn't their own.
- **Verification:** All participants fill out the **EU Survey on Justice, Rights and Values** to document their involvement and the success of the outreach.

